NISTIR 4651

Government Network Management Profile (GNMP): Public Review Version of Proposed FIPS

Robert Aronoff
Kevin Brady
Michael Chernick
Jim Fox
Karen Hsing
Kevin Mills
Fran Nielsen

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards
and Technology
Computer Systems Laboratory
Gaithersburg, MD 20899

U.S. DEPARTMENT OF COMMERCE
Rockwell A. Schnabel, Acting Secretary

NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
John W. Lyons, Director

NIST

NISTIR 4651

Government Network Management Profile (GNMP): Public Review Version of Proposed FIPS

Robert Aronoff
Kevin Brady
Michael Chernick
Jim Fox
Karen Hsing
Kevin Mills
Fran Nielsen

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards
and Technology
Computer Systems Laboratory
Gaithersburg, MD 20899

January 1992

U.S. DEPARTMENT OF COMMERCE
Rockwell A. Schnabel, Acting Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
John W. Lyons, Director

Government Network Management Profile (GNMP):

Public Review Version of Proposed FIPS

May 31, 1991

This version of the GNMP has been circulated for public review comment and is expected to change as a result of accommodating those comments. Expected changes include, but are not limited to, changes related to alignment with the latest network management International Standards and Implementors Agreements on those standards. The sections on managed objects (MOs) may change as a result of harmonization with other MO definition groups. The FIPS version of this document is expected in June 1992. For information, contact: Ms. Fran Nielsen, Manager, Network Management Group, NIST/Computer Systems Laboratory, Gaithersburg, MD 20899.

Robert Aronoff
Kevin Brady
Michael Chernick
Jim Fox
Karen Hsing
Kevin Mills
Fran Nielsen

National Institute of Standards and Technology

(NIST)

Government Network Management Profile

(GNMP)

Contents

List of Figures

Preface

This is the Federal Government procurement profile for network management products.

Section 1 contains introductory material, the purpose and scope of the profile, and the sources of the specifications contained in the profile. Section 2 describes how to use this profile. Section 3 provides a tutorial overview of the OSI management standards included in this profile. Section 4 contains the specifications for the network management profile, while Section 5 contains general statements on conformance and testing.

This profile will change with improvements in technology and with the evolution of network management standards. Appendix A specifies future work items planned to enrich the profile. Appendix B provides definitions for the acronyms used in this document. Appendix C provides a list of the object and attribute names, along with document references for all objects included in Version 1 GNMP. The suggested name bindings for each group of managed objects are included in Appendix D.

Glossary

The terms defined below are used frequently throughout this profile and are defined here to aid the reader. The Basic Reference Model, ISO/IEC 7498 [BRM], may be referenced for other terms appearing in this document.

Acquisition Authority	An individual or team who, under Federal law and acquisition regulations, has the authority to enter into, administer, and/or terminate a government contract.
Agent	An application, making use of systems management services, which, for a particular exchange of systems management information, has taken an agent role.
Agent Role	An application, making use of systems management services, taking an agent role is capable of performing management operations on managed objects and of emitting notifications on behalf of managed objects.
Allomorphism	The ability of a managed object of a given class to resemble one or more other object classes.
Containment	A structuring relationship for managed objects in which the existence of a managed object is dependent upon the existence of a containing managed object. The contained managed object is said to be the **subordinate** managed object and the containing managed object the **superior** managed object.
Inheritance	The conceptual mechanism by which attributes, notifications, operations and behaviour are acquired by a subclass from its superclass.
Managed Object (MO)	The OSI Management view of a resource within the OSI environment that is subject to management, such as a layer entity, a connection or an item of physical communications equipment. A managed object is the abstracted view of such a resource that represents its properties as seen by (and for the purposes of) management.
Managed Object Class	A named set of managed objects sharing the same set of attributes, notifications and management operations.
Management Information	The information within an open system which may be transferred or affected through the use of management protocol(s).
Manager	An application, making use of systems management services, which, for a particular exchange of systems management information, has taken a manager role.
Manager Role	An application, making use of systems management services, taking the manager role is capable of issuing management operations and of receiving notifications.

Name Binding	A relation between managed object classes for the purpose of naming.
Naming Tree	A hierarchical arrangement of managed objects where the hierarchy is organized on the basis of the containment relationship. A managed object used to name another managed object is higher in the hierarchy than the named object. The naming managed object is referred to as being the **superior** of the managed object, which is referred to as the **subordinate**.
Notification	Information emitted by a managed object relating to an event that has occurred within the managed object.
Open Systems Interconnection (OSI)	OSI is concerned with the exchange of information between possibly heterogeneous systems, and deals with the capability of those systems to interwork to achieve common (distributed) tasks. OSI is not concerned with the internal functioning of each individual system.
OSI Management	The facilities to control, coordinate and monitor the resources which allow communications to take place in the OSI environment.
Protocol	In the Open System Interconnection reference model, the communication functions are partitioned into seven layers. Each layer, N, provides a service to the layer above, N+1, by carrying on a conversation with layer N on another processor. The rules and conventions of that N-layer conversation are called a protocol.
Requests For Proposals (RFP)	Requests For Proposals are documents issued by the government to request bids for products or services.
Systems Management Application-Entity (SMAE)	An application-entity for the purpose of systems management communication.
Systems Management Function (SMF)	A part of systems management activities which satisfies a set of logically related user requirements.
Systems Management Service	A named set of service primitives that provide a service for use in systems management.

1. Introduction

The Government Network Management Profile (GNMP) is the standard reference for all Federal Government agencies to use when acquiring Network Management (NM) functions and services for computer and communications systems and networks.

To provide background information on network management (NM), this section, first, discusses the urgent need for integrated NM tools; then examines the status of NM standards and of implementation agreements (IAs). Next, the purpose and scope of the GNMP and its applicability to federal government procurement are described. Lastly, the approach taken for the development of the GNMP is presented, the sources of specifications are listed, and the relationship between the GNMP and the Government Open Systems Interconnection Profile (GOSIP) is explained.

1.1. Need for Integrated Tools for Network Management

Network management is vital to the practical operation of large networks. Usage of network services is affected by the availability and effectiveness of network management capabilities. Presently, network control and monitoring activities, when available, are accomplished primarily through the use of proprietary tools and/or software in a piecemeal, non-integrated manner. Network operations managers categorize their problems in one of two ways. In one situation, NM tools come from different vendors and function in proprietary methods. However, they do not interoperate in an integrated manner. This increases cost and inefficiency in managing networks. In the other situations, NM tools come from a single vendor and, consequently, do operate in an integrated manner. However, the network owner, in order to obtain this integration, may not be able to procure management products from other vendors, even when such products might be less costly or more desirable technically. The need for products to manage components of multi-vendor networks in an integrated manner is quite real, well-documented, and urgent; and the need is increasing. The U.S. Government, with its multiplicity of computer systems and communications networks, requires integrated NM tools from multiple vendors.

1.2. Status of OSI Network Management Standards and Implementors Agreements

The Open Systems Interconnection (OSI) management standards, while currently at an intermediate stage of their development, are maturing rapidly. The ultimate goal of these standards is to enable the development of interoperable, multi-vendor products for the management of computer and communications systems and networks. Key areas of management standardization are architecture, protocols, systems management functions, and the structure of management information. The Common Management Information Services and Protocol (CMIS/P) standards [CMIS] [CMIP] have now become International Standards (IS). Many other needed management standards are still at the Draft International Standard (DIS) status. However, these DISs, available at the beginning of 1991, compose a subset of management standards that make it possible for vendors to build useful systems to meet some immediate network management requirements. Still other standards are planned or proposed (for example, the Software Management Function and the Generic Managed Objects Standard), but have not yet been added to the International Organisation for Standardisation/International Electrotechnical Committee (ISO/IEC) schedule for standardization.

Another important aspect of network management standards activity is the development of Implementation Agreements (IAs). The Network Management Special Interest Group (NMSIG) of the OSI Implementors' Workshop (OIW) (sponsored by NIST and the IEEE Computer Society) is developing IAs based on the emerging NM standards. These agreements are being developed in phases that align with the ISO/IEC standards as they progress from CD (Committee Draft) to IS. The OIW NM Phase 1 IAs became stable in December 1990. [STABLE]

1.3. Purpose

Within the government, system and network management can best be accomplished by using a single profile to specify all the standards to which NM products must comply. In the absence, at present, of a complete set of mature standards for NM, a set of initial NM specifications that contains a useful subset of the planned system and network management functionality provides an interim solution to meet some high priority requirements. NIST is, therefore, proposing a Federal Information Processing Standard (FIPS) for network management. This FIPS is called the Government Network Management Profile (GNMP).

The GNMP is being developed in phases. Version 1 GNMP specifies an initial, useful set of standards to permit an Acquisition Authority to issue unambiguous procurement requests for standard, interoperable NM products capable of operating over networks using standard protocols.

1.4. Scope

The GNMP specifies the common management information exchange protocol and services, specific management functions and services, and the syntax and semantics of the management information required to support monitoring and control of network and system components and their resources.

Version 1 GNMP specifies: 1) the Common Management Information Services and Protocols (CMIS/P), [CMIS and CMIP], 2) the management information definitions as specified in section 4 of the GNMP, and 3) the following five systems management functions (SMFs).

- Object Management Function
- State Management Function
- Attributes for Representing Relationships
- Alarm Reporting Management Function
- Event Report Function

For detailed specifications of standards and IAs, see section 4 of the GNMP. For brief descriptions of the standards included in this profile, see section 3. The latest versions of all the NM standards included in Version 1.0 GNMP are intended to be referenced in the GNMP when it is published as a FIPS. The standards for the Structure of Management Information and for the systems management functions specified in this document are expected to become IS before Version 1.0 GNMP is published.

1.5. Applicability

The GNMP must be used by Federal government agencies when procuring network management products and services which provide equivalent functionality to the system and network management standards referenced in this document.

1.6. Approach

The GNMP is being developed in phases. This document specifies the initial phase of the GNMP. Additional management capabilities and managed objects will be included in subsequent releases of the

profile. Eventually, as the NM standards all reach technical maturity, the GNMP will embrace the full set of management functionality.

For the development of the initial phase, a three-step approach was taken:

(1) analysis of NM requirements ,

(2) comparison of requirements with emerging standards and implementors' agreements, and

(3) proposals to resolve any essential, unmet needs/requirements.

The purpose of requirements analysis was to assure that the GNMP will address real needs within the U.S. Government. Network management requirements were collected from a survey, conducted by NIST in the summer of 1990, of federal agencies. Survey results indicated that management of local area networks (LANs), as well as the bridges that interconnect them, represents a key NM requirement. Furthermore, access control to NM information and NM commands was considered to have the highest priority among all the network management security requirements.

The NM requirements identified from the survey were compared with the emerging NM standards and IAs. An obvious need recognized by the comparison study was the requirement for management information definitions. Although some support management information (MI) has been defined by the International Organisation for Standardisation/International Electrotechnical Committee (ISO/IEC) NM working group and they have specified a set of guidelines and templates for defining MI, they have not specified the definitions of particular MI to be monitored and controlled. Various standards-making groups and implementors forums are currently developing definitions of MI pertinent to their specific areas of expertise and standardization by using the standard definition templates that ISO/IEC has developed.

Defining management information not only requires in-depth knowledge of the specific subject areas to which the management information belongs, but also requires understanding of the management information model and the standard templates. Consequently, it takes extended development time to define specific management information. For inclusion in the GNMP, management information has been divided into three groups corresponding to the three phases of the development of the GNMP. The focus of each phase has been determined in accordance with the prioritized NM requirements obtained from the survey. The Phase 1 GNMP focuses, mainly, on definitions of management information pertaining to implementations that perform layer 1 and 2 functions. Appendix A indicates the areas of concentration for defining Phases 2 and 3 management information.

1.7. Sources of Specifications

The primary source of specifications in the Version 1 GNMP is part 18 of the OIW Stable Implementation Agreements, December, 1990 [STABLE]. This source provides implementation specifications for network management based on the service and protocol standards issued by the ISO/IEC.

The GNMP is intended to be a complete profile, specifying all that is necessary to assure that a NM system procured in accordance with its specifications will interoperate and provide services generally useful for network managers (operators). However, since the OIW IAs continue to evolve and the NM IAs are still incomplete, additional sources of specifications are needed in order to achieve the minimum required capabilities. Additional sources of specifications for the Version 1 GNMP include those standards committees and implementors groups which have developed definitions of needed management information:

- Management Information Library (MIL) [MIL],
- NMSIG contribution to IEEE 802 standards [NM802],
- IEEE 802.3 HUB management [HUB],
- ANSI X3T9.5 FDDI SMT [FDDI],
- ANSI T1M1.5 [T1M1],
- ISO/IEC SC6 [SC6], and
- NIST contribution of Modem definition to NMSIG [MODEM].

1.8. GOSIP and GNMP

The Government Open Systems Interconnection Profile (GOSIP) is cited in the GNMP to specify the protocol stack upon which management information can be conveyed. The GOSIP also specifies services, such as File Transfer, Access and Management (FTAM), Message Handling System (MHS), and Virtual Terminal (VT), that can be used to support network management applications. Future versions of the GNMP will enable management of more GOSIP components (e.g., transport connections and key exchanges.) Future versions of the GOSIP will cite the GNMP to specify the management protocols, services, and information needed to facilitate interoperable multi-vendor management of GOSIP-compliant systems. As both the GNMP and the GOSIP mature, it is expected that they will continue to cross reference the latest versions of each other.

2. How to Understand and Use the GNMP

Business and governments continue deployment of voice and data communications networks at an increasing pace. The local area network (LAN) market in the U. S. grew 26% in 1990 to $2.6B, and 4 million network interface cards were shipped. The aggregate U.S. market for private branch exchanges (PBXs) and digital switches reached $6B in 1990. The deployment of these networking devices is generating intense pressure for suppliers to provide network management products as well. Suppliers are responding with capable, but incompatible, network managers. The result in most large organizations today is a loose confederation of multi-vendor systems managed by a variety of network management products. The situation in a typical company is illustrated in Figure 2.1. In the example, five different terminals are required to manage all the network assets, and nowhere is an integrated view available.

The solution to this dilemma depends upon an integrated network management system. For the company illustrated in Figure 2.1, a solution such as is shown in Figure 2.2 might be feasible. All five network managers (the two LAN managers, the wide-area network (WAN) manager, the telecommunications manager, and the PBX manager) remain in place, using proprietary means to manage specific resources. Four network management integrators have been added: one integrates the LAN managers, one integrates the telecommunications managers, one integrates the WAN manager and the LAN integrator, and one integrates the telecommunications and data communications integrators. Implementation of such a hierarchical network management system requires a standard for network management information exchange between integrators, and between integrators and managers. In Figure 2.2, interfaces requiring such a standard are shown with broken lines connecting the label "GNMP".

The Government Network Management Profile (GNMP) specifies a standard for the exchange of management information between integrators and between integrators and managers. The GNMP specification can also be used between managers and network elements, should the network elements possess sufficient computing capability. The scope of the GNMP encompasses a set of protocols for multi-vendor communications, a set of general-purpose management functions, and a standard set of managed object definitions. This scope addresses only the exchange of management information in a standard way in order to achieve integration of management systems and components made independently by a variety of suppliers.

Other important issues are outside the scope of the GNMP. Consider, for example, the analysis of management information. For any operational network management system, raw management data must be collected, stored, calculated, and correlated to provide useful outputs for network planning, fault prediction, and billing. Requirements in these areas are outside the scope of the GNMP and must continue to be specified directly by the Acquisition Authority. Human-machine Interface (HMI) is also outside the scope of the GNMP. The Acquisition Authority must continue to specify any requirements regarding presentation and ease of use. The usual issues of configuration and sizing of network management components are also outside the scope of the GNMP. The Acquisition Authority must continue to plan the deployment and sizing of specific integrators and managers in accordance with operational requirements. The GNMP, then, addresses a single, significant network management integration problem: interoperability between network management components.

Phase 1 GNMP includes an international standard common management information protocol (CMIP) and five general management support functions. More management support functions will be included in future phases as these functions become available. Phase 1 GNMP incorporates managed object definitions for network interfaces, including LANS, X.25, Integrated Services Digital Networks (ISDN), Fiber Distributed Data Interface (FDDI), modems, bridges, and links. A rudimentary capability to manage Open Systems Interconnection (OSI) routers and transport connections is also included. Additional managed objects are planned in phases as shown in Appendix A.1. The eventual scope of the GNMP will be extended to include system management objects for applications, services, operating

systems, and database systems. Phase 1 GNMP includes optional methods of authentication. These optional authentication methods are provided for interim use in the absence of standard approaches to network management security. Regarding access control, the GNMP assumes that a properly authenticated user should have access to any management information available. Future phases of the GNMP will provide finer-grained access control as appropriate standards are agreed.

The GNMP builds on the Government Open Systems Interconnection Profile (GOSIP). In fact, the GNMP includes the GOSIP Version 2.0 by reference. The GOSIP specifies the lower layer (1-6) protocols to provide basic interoperability in support of CMIP. In addition, the GOSIP Version 2.0 provides three applications that might be useful in a general purpose network management solution. The File Transfer, Access, and Management (FTAM) application facilitates the transfer of bulk information, such as routing tables, billing records, audit trails, and configuration data. The Virtual Terminal (VT) application enables remote login to network management systems; thus, allowing a network operator to execute proprietary network management tools and diagnostics. The Message Handling System (MHS) permits network operators to exchange messages with each other while attempting to diagnose or correct network problems. MHS can also be employed to alert users about network status changes. Future phases of the GNMP will include managed object definitions for layers three through seven for GOSIP-compliant end systems and for layer three for GOSIP-compliant intermediate systems. Thus, the GNMP and the GOSIP are tied intimately, cross-referencing each other as required.

With the foregoing background information, an Acquisition Authority can understand how to use the GNMP to specify interoperable network management interfaces for components in a network management system. First, the Acquisition Authority must develop a plan for partitioning network management responsibilities among network managers and for interconnecting the managers through network integrators. The specific number, location, scope, and size of the managers and integrators will depend on the operational requirements of the Acquisition Authority. Second, the Acquisition Authority must decide whether or not authentication is required, and if so, which specific option is needed. Third, the Acquisition Authority must determine which optional GOSIP applications, if any, are required for each manager and integrator. Fourth, the Acquisition Authority must select the managed objects required to be supported for each manager and integrator. For each selected managed object, the Acquisition Authority must determine if any of the optional attributes are required to be supported. Fifth, the Acquisition Authority must define the relationships between instances of managed objects needed to support the operational requirements. Having made these decisions, the Acquisition Authority can use the GNMP to specify protocol requirements for each manager and integrator, so that interchange of management information can be achieved. Beyond the GNMP, the Acquisition Authority must specify man-machine interface requirements, management data analysis requirements, system and component capacity and performance requirements, and any other requirements.

In sum, the GNMP is a useful tool to specify interfaces between managers and integrators to enable exchange of management data and execution of management functions when the managers and integrators might be provided by a variety of suppliers. The GNMP permits significant flexibility regarding many engineering issues, and can be tailored to some degree for specific requirements. This initial phase of the GNMP is simply a beginning; future enhancements, as outlined in Appendix A, are already foreseen.

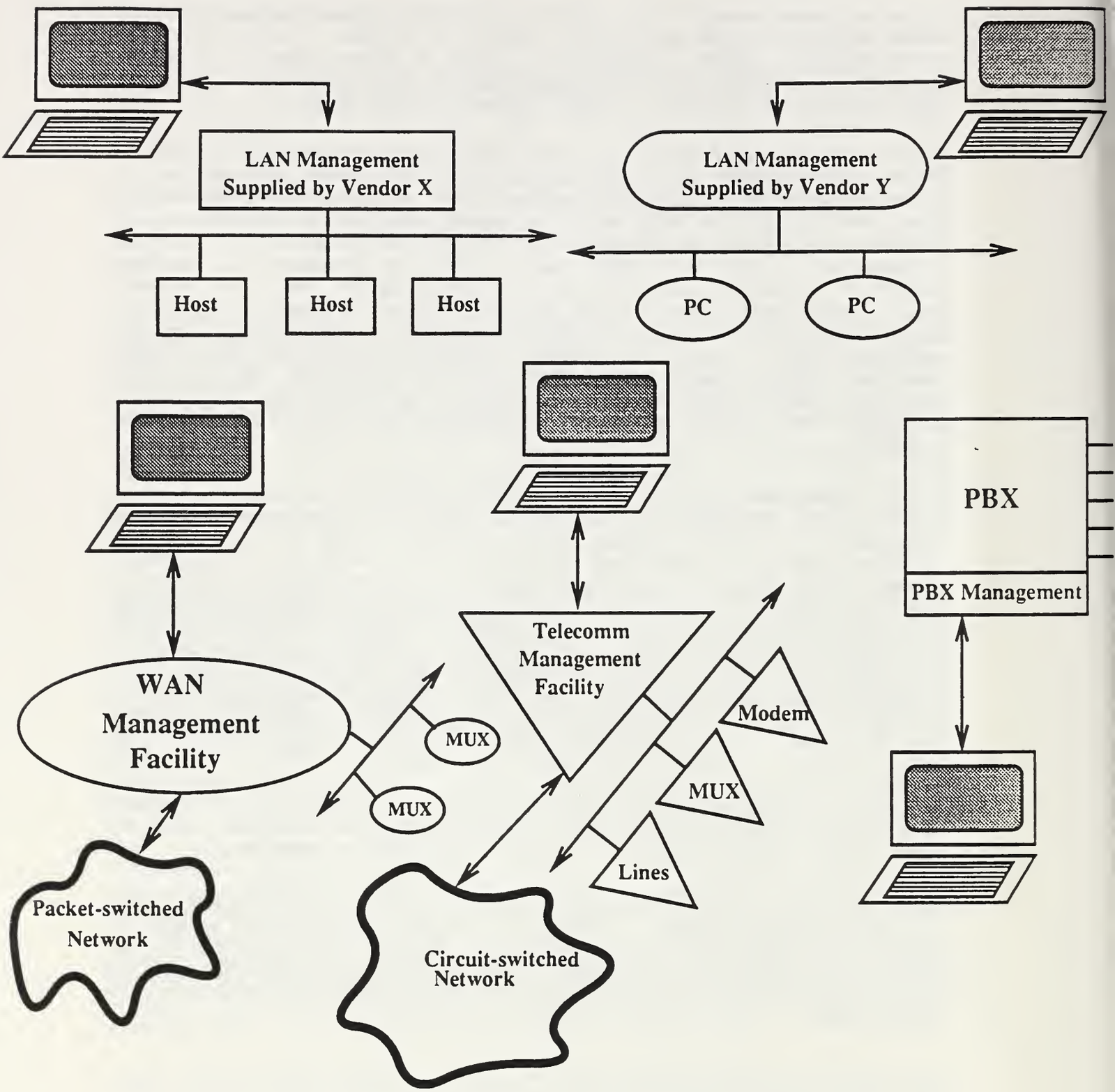


Figure 2.1 Network Mangement in a Non-integrated Manner

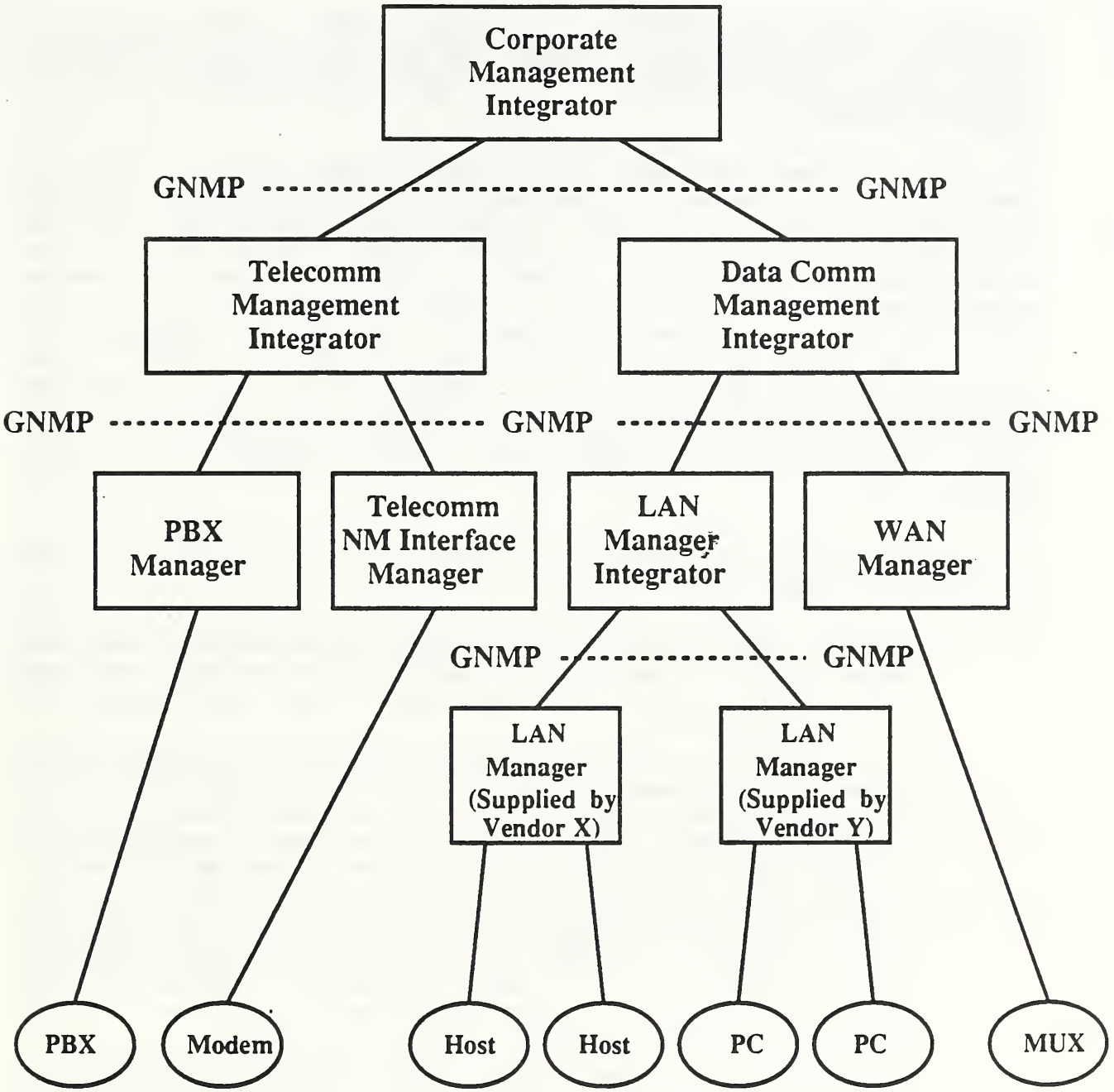


Figure 2.2 Integrated Network Management Using GNMP

3. Description of Network Management Standards

This section provides an overview of the OSI management standards. First, the organization and interrelationships of these standards are explained; then each standard is briefly described. The information in this section is intended to be tutorial. The specifications of standards selected for this profile are in section 4.

The international standards for the management of networks are rapidly approaching maturity. These standards jointly provide a foundation for the development of interoperable NM products. The primary goal for developing interoperable NM products is to allow network managers to remotely monitor and control network resources residing on network components developed by different vendors. In order to accomplish this, there must be a common method for transferring the management commands and management information; and there must be a common view of management information. To exchange management commands and information, OSI management defines a standard management protocol, known as the Common Management Information Protocol (CMIP). To provide a standard representation of management information, a set of standards called the Structure of Management Information (SMI) has been developed. In addition to CMIP and SMI, a set of standards, known as the Systems Management Functions (SMFs), is also being developed to define specific services to support network management. These services are for configuration, fault, security, performance and accounting management.

As specified in the Systems Management Overview (SMO) [SMO], OSI management standards are subdivided into four groups:

(1) *Standards specifying the architecture and organization of OSI Management* - This group of standards includes the Management Framework [FRMWK] and the Systems Management Overview [SMO]. Presently, the Management Framework is an international standard while the SMO has reached DIS.

(2) *Standards for the communication of management information* - This group of standards includes the Common Management Information Services (CMIS) [CMIS] and the Common Management Information Protocol (CMIP) [CMIP]. These two standards specify how the exchange of management information between two open systems is accomplished. CMIS and CMIP are ISs. Subsection 3.1 of this GNMP describes the CMIS and CMIP standards.

(3) *Standards relating to the structure of management information (SMI)* - The standards in this group specify the syntax of information which is transferred for management purposes. The standards that support the specification of management information are: the Management Information Model [MIM], the Definition of Management Information [DMI], and Guidelines for the Definition of Managed Objects [GDMO]. These standards have reached the DIS status. Subsection 3.2 briefly describes each of these standards.

(4) *Standards for systems management functions (SMFs)* - The standards in this group define the services and, if appropriate, the functional units and generic definitions of managed objects required for each specific systems management function. The SMF standards are at various stages of development, ranging from working proposals to committee drafts to DISs. The Object Management Function [OMF], the State Management Function [STMF], Attributes for Representing Relationships [ARR], the Alarm Reporting Function [ARF], the Event Report Management Function [ERMF] and the Log Control Function are DISs. Other SMFs (such as the Workload Monitoring Function, the Summarization Function and Objects and Attributes for Access Control) are not yet DIS. Subsection 3.3 describes the five SMFs included in the phase 1 GNMP.

Other standards related to network management security are currently being developed by various standards groups. Section 3.4 discusses the security options presently available for network

management.

Taken together, these NM standards define aspects of NM that must be implemented in a standard way to allow interoperable, multi-vendor management. Figure 3.1 illustrates how these management standards fit in the application layer structure in an open system (for detailed description of the architecture of the application layer, see the international standard for Application Layer Structure [ALS]). Those non-standardized, but generally required, NM elements, such as human-machine interface, are also included in the illustration and are designated as recommended elements. The application layer standards, such as FTAM, that may be used by network management applications are included as well and are designated as optional elements.

3.1. Management Communications

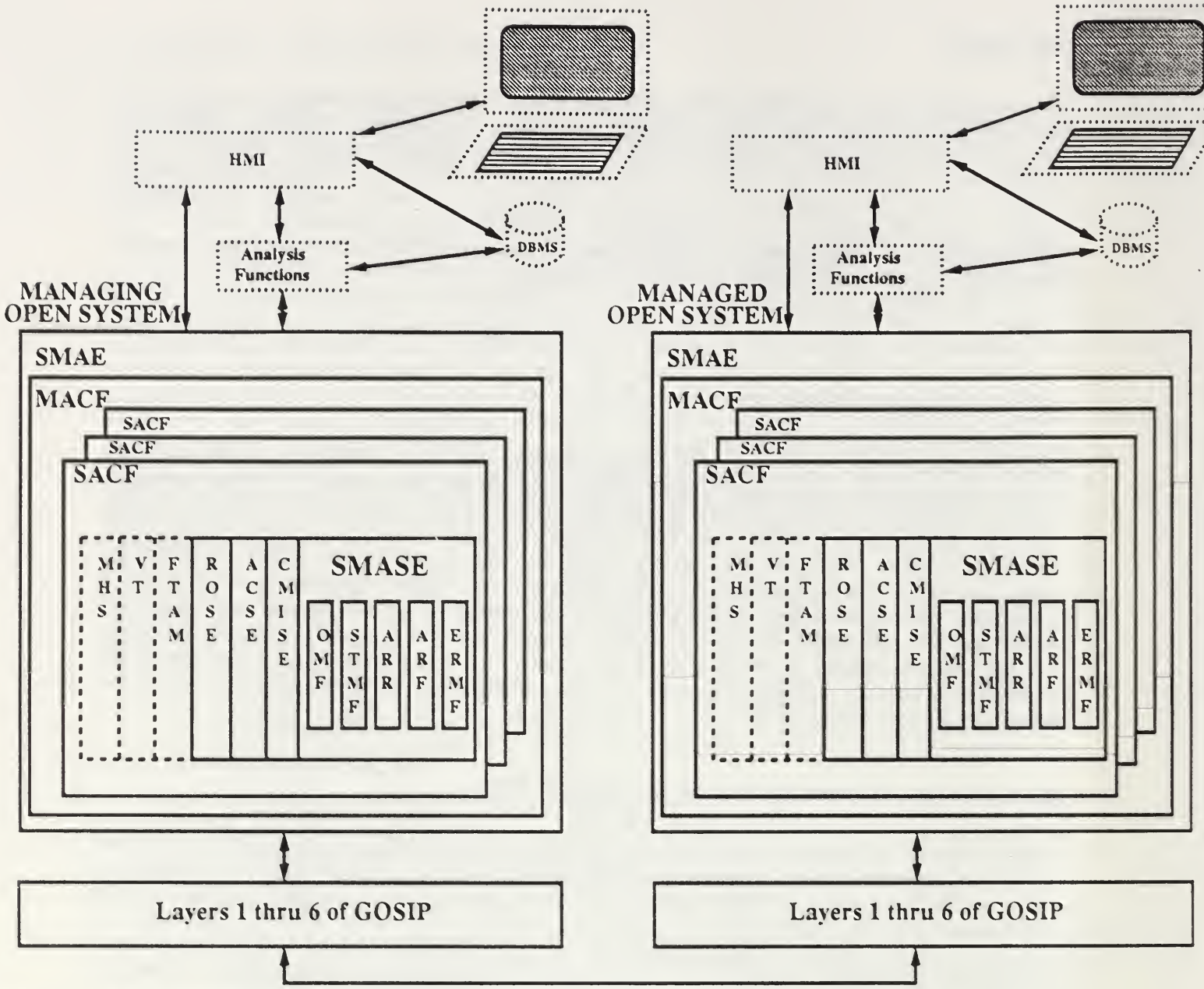
Network management requires the ability to communicate management information and commands between open systems. The management communication protocol and service provide an information transfer mechanism, mutually agreed by peer participating management entities. The service and protocol developed by ISO/IEC for OSI systems management are the Common Management Information Service (CMIS) and the Common Management Information Protocol (CMIP). CMIP is the application layer protocol used in the OSI environment to transfer management commands and information between open systems. CMIP specifies the makeup of the management messages, while CMIS specifies the service interface to CMIP. Although not stated in these particular standards, normally in any example of management communication, the management entity on one end of the association assumes a manager role, while the peer management entity on the other end of the association assumes the agent role.

3.1.1. Common Management Information Protocol (CMIP)

CMIP provides a commonly understood format for the transfer of management information and commands between the peer management entities. Typically, one of the peers acts in a manager role and one acts in an agent role during management communications. CMIP specifies the generic transfer mechanism needed by the systems management functions (e.g., OMF, STMF). The types of management information and commands that are exchanged using CMIP take the general form of event notifications, information or action requests, and responses, containing either the requested information or some indication as to why the request failed.

3.1.2. Common Management Information Services (CMIS)

CMIS provides a full range of services by means of a small number of basic service primitives. The major ones are: 1) M-GET, a read operation to retrieve attribute values of managed objects; 2) M-SET, a write operation to permit the setting of managed object attribute values; 3) M-EVENT-REPORT, an operation to transmit relevant information concerning significant predefined occurrences on one system (e.g., an agent) which are to be reported to another system (e.g., its manager); and 4) M-ACTION, an operation intended to remotely invoke a predefined management activity on a managed object located on the target system. The ability to establish new management information object instances, or to remove no longer needed management information object instances, is supported by the CMIS service primitives, M-CREATE and M-DELETE, respectively.



ARF: Alarm Reporting Function
ACSE: Association Control Service Element
ARR: Attributes for Representing Relationships
CMISE: Common Management Information Service Element
DBMS: Database Management System
ERMF: Event Reporting Management Function
FTAM: File Transfer, Access and Management
GOSIP: Government OSI Profile
MACF: Multiple Association Control Function
MHS: Message Handling System
HMI: Human Machine Interface
OMF: Object Management Function
ROSE: Remote Operations Service Element
SACF: Single Association Control Function
SMAE: Systems Management Application Entity
SMASE: Systems Management Application Service Element
STMF: State Management Function
VT: Virtual Terminal

LEGEND

..... Recommended but not standardized

- - - - - - - Optional

Figure 3.1 Components of Interoperable Management Open Systems

The intent of the CMIS service primitives is to allow the management service user: 1) to specify the management operation (command) being transmitted; 2) to pass appropriate support information; 3) to pass result or error information; 4) to identify the particular managed object/attribute/action/event to be operated upon, either by directly naming the specific object instance or by specifying criteria by which an appropriate set of objects can be selected (i.e., through the use of "scoping," to select potential object targets, and "filtering," to select the actual targets which satisfy a specified set of conditions); 5) to identify the particular instance of management communication; 6) to pass access control information; and 7) to specify when operations and events occurred.

CMIS capabilities are partitioned into functional units which can be negotiated between peer management applications communicating over a given association. The resulting negotiated agreement limits the range of management communication allowed on that association. The kernel functional unit of CMIS includes all the basic service primitives mentioned above. This kernel functionality can be augmented by negotiating functional units which make available services within CMIS for "scoping" and "filtering," in order to designate sets of objects to be operated on and to allow for multiple replies in such cases. An additional functional unit makes available the extended use of presentation layer services.

3.2. Management Information

To provide interoperability among network management systems, each system must have a common "view" of management information. This involves first assuring that the abstract conceptual view of management information is consistent. Within this consistent management information model, then, management information must be defined in a consistent way. Finally, a registration methodology and repository for management information definitions is required, so that general access is provided to these definitions.

Several international standards exist to facilitate a common view of management information. These standards provide: 1) an overview and model of management information, 2) a generic approach to and format for defining management information, and 3) certain specific definitions of managed objects to support network management functions. The following three subsections expand upon each of these documents. The fourth following subsection discusses issues related to the actual definitions of management information (managed objects) and repositories for management information definitions.

3.2.1. Management Information Model (MIM)

The Management Information Model [MIM] describes an object-oriented model of management information. This model divides management information into managed objects, their attributes, the management operations that can be performed upon them, and the notifications that they can emit. The set of managed objects in an open system, together with their attributes, constitute that open system's management information base. Using object-oriented principles, the management information model defines key concepts such as inheritance, allomorphism, containment and naming, as they relate to managed objects.

3.2.2. Guidelines for the Definition of Management Objects (GDMO)

The Guidelines for the Definition of Management Objects [GDMO] specifies how management information definitions shall be defined, what notational tools are to be used in such definitions, and what documentation structure is to be used for managed object class definitions. Included in GDMO are

templates for management information definitions. These templates provide common, detailed descriptions for defining managed object classes, name bindings, attributes, actions and notifications.

3.2.3. Definition of Management Information (DMI)

The Definition of Management Information [DMI] defines often used managed object classes, packages, attribute types, specific attributes, action types, parameter types, and notification types. DMI also specifies compliance requirements placed on other standards that make use of the definitions.

DMI provides generic definitions that support systems management functions and can thus be incorporated in other management information definitions. These definitions may also be used in other standards to specify objects, attributes, notifications and action types.

3.2.4. OIW Management Information Library (MIL)

One of the key issues regarding management information is how and where to register and maintain management information definitions. Management information, for classes of network resources, needs to be defined, registered, and ultimately placed into standard libraries so that common views of network resources will be available to all NM users and implementors. To date, however, although several are planned, few standard libraries are available. To fill this void, the OIW NMSIG has developed a Management Information Library (MIL) which provides a core set of management information definitions. However, considering the focus of the Phase 1 GNMP on layers 1 and 2, the managed objects in the MIL, regrettably, are insufficient to enable management of LANs and other devices which provide layer 1 and 2 functionality. In order to augment the MIL definitions and to provide the necessary managed object definitions to support management of layer 1 and 2 functionality, additional managed object definitions are being included in the GNMP. These additional definitions include managed objects (MOs) being developed by IEEE 802, ANSI X3T9.5 FDDI, ANSI T1M1.5, ISO/IEC SC6 for the Network layer, and NMSIG's contributions to IEEE 802 standards. A set of MOs to support modems is also included. Appendix C provides an overview of these MOs and their attributes by listing the object and attribute names, along with document references. The suggested name bindings, for each group of MOs, specified by the relevant standards committees are included in Appendix D. Name bindings are used to name instantiations of the managed objects, known as managed object instances. To obtain greater detail about these MOs and their attributes, consult the listed references for the actual definitions. MOs that are included in the Phase 1 GNMP will be registered when the GNMP is promulgated as a Federal Information Processing Standard (FIPS).

3.3. Systems Management Functions and Services

To develop functions for the support of systems management, ISO/IEC has partitioned systems management activities into five Specific Management Functional Areas (SMFAs): configuration management, fault management, performance management, security management, and accounting management. Within each of these SMFAs, ISO/IEC groups are developing standards for functions (including requirements, models, and services) for the management of networks. Because of overlap among requirements of the SMFAs, management functions developed to satisfy the needs of one SMFA can often be used in support of other SMFAs. The functions developed by the SMFA groups of ISO/IEC are known as Systems Management Functions (SMFs). Five of these SMFs are included in the Phase 1 GNMP: Object Management Function (OMF), State Management Function (STMF), Attributes for Representing Relationships (ARR), Alarm Reporting Function (ARF) and Event Report Management Function (ERMF). The following SMFs are under development by ISO/IEC but are not included in the Phase 1 GNMP: Log Control Function (LCF), Security Alarm Reporting Function (SARF), Security Audit Trail Function (SATF), Objects and Attributes for Access Control (OAAC), Accounting Metering Function (AMF), Workload Monitoring Function (WMF), Test Management Function (TMF), and

Summarization Function (SF). The intention of the standards community is to develop additional SMFs as needs are identified. As these additional SMFs reach maturity, they will be considered for inclusion in future phases of the GNMP. Brief summaries of each of the first five SMFs are presented in the sub-sections that follow. At the time the GNMP is promulgated as a FIPS, if the SMF's included in the Version 1 GNMP have reached IS status, these IS's (instead of SMF DIS's) will be included in the final Version 1 GNMP. The OIW NMSIG is expected to adopt the SMF IS's as soon as they are available.

3.3.1. Object Management Function (OMF)

Managed objects provide a view of system resources that may be managed using OSI management protocols. The OMF enables a management user to create, delete, examine or modify characteristics of managed objects. The OMF describes the following services: reporting of the creation and deletion of managed objects, reporting of name changes of managed objects, and reporting of changes of attribute values of managed objects. The OMF also describes, so called, "pass-through" services which map directly to CMIS. These include: creating and deleting managed objects, performing actions upon managed objects, changing attribute values, reading attribute values, and reporting events. For details on each of these services see DIS 10164-1 [OMF].

3.3.2. State Management Function (STMF)

The State Management Function defines three attributes whose values are used to indicate or control the state of a resource represented by a managed object. These attributes are: operational state, usage state, and administrative state. The value of the operational state attribute indicates whether or not the resource is physically installed and/or working. The value of the usage state attribute indicates whether the resource is active, and if it is, whether the resource has spare capacity for additional users. The value of the administration state attribute indicates whether the use of a resource is permitted or prohibited. The value of the administrative state may be set through the use of management services. The STMF defines generic attributes and operations that can be part of any managed object definition in order to provide a standardized OSI Management technique for dealing with management states. The STMF provides the management user the ability to examine states, to be notified of changes in state, to monitor overall operability and usage of resources in a consistent manner, and to control the general availability of specific resources. For details on the factors affecting the states of a managed object and the set of attributes and notifications (see section 3.3.5) related to State Management see DIS 10164-2 [STMF].

3.3.3. Attributes for Representing Relationships (ARR)

According to the Attributes for Representing Relationships document, managed objects may be related in one of the following three categories of relationships: containment relationships, reciprocal relationships, and one-way relationships. Containment relationships are defined in DIS 10165-1 [MIM]. Reciprocal and one-way relationships are defined in DIS 10164-3 [ARR]. The ARR standard provides a model for specifying relationships among managed objects and indicates which attributes, defined in DIS 10165-2 DMI [DMI], are to be included in managed object definitions for the purpose of representing these relationships. Relationships are used to provide a set of rules governing how one part of an open system may affect other parts of the system.

In addition to describing the nature and types of managed object relationships and how they are represented, ARR describes the monitoring and controlling of these relationships. Beyond the basic management capabilities of reading and setting attribute values which represent these relationships, ARR defines a service which specifies how notifications (see section 3.3.5) of relationship changes are to be reported. A description of the different types of relationships and the generic relationship

attributes is provided in DIS 10164-3 [ARR].

3.3.4. Alarm Reporting Function (ARF)

The ARF specifies particular categories of alarms as well as a mechanism for communicating these alarms between peer management users. The ARF [ARF] specifies the following five basic categories of alarms along with their parameters and semantics: communications, quality of service, processing failure, equipment, and environmental. Included within the description of these alarm types are parameters and semantics. Some examples of alarm causes are: queue size exceeded, retransmission rate excessive, and out of memory.

The alarms discussed in the ARF are particular types of notifications (see section 3.3.5) which convey information about detected faults and abnormal conditions. The ARF, therefore, supports the network management capability to detect faults, or those abnormal conditions generally leading to faults, as early as possible, and preferably before problems are noticed by the network users. For details on each of these categories of alarms see DIS 10164-4 [ARF].

3.3.5. Event Report Management Function (ERMF)

Management events indicate that some measurable activity has occurred in a network management system. When an event has occurred within a managed object, a notification is emitted by the object. Notifications are passed through discriminators, which specify conditions that must be satisfied prior to generating an event report. The ERMF standard [ERMF] discusses discriminators and provides the management user the following capabilities: the definition of a flexible event report control service, the specification of destinations to which event reports are to be sent, the specification of a mechanism to control forwarding of event reports, the ability for an external managing system to modify conditions used in the reporting of events, and the ability to designate a backup location to which event reports can be sent if the primary location is not available. For details on each of these capabilities see DIS 10164-5 [ERMF].

3.4. Management Security

3.4.1. Services

The GOSIP identifies the primary services required for security in an open system. These services are:

- authentication (verifies the identity of communicating peer entities),
- access control (allows only authorized communication and system access),
- data confidentiality (protects data against unauthorized access),
- data integrity (protects data against unauthorized modification, insertion, and deletion), and
- non-repudiation (provides proof of the origin or receipt of data).

The Network Management SIG, of the OIW, has identified the following security services, as qualified below, as the primary requirements for network management security:

- authentication - peer entity and data origin authentication,
- access control,
- confidentiality - connectionless confidentiality,

- integrity - connectionless integrity.

Since not all systems will require all the security services, and not all these services will be available in the immediate future, the Network Management SIG has prioritized these services with regard to their general usefulness and urgency. Highest priority has been given to access control. In addition, because access control is so closely related to and dependent upon authentication, authentication was also given a high priority (i.e., it must be verified that a person or process is in fact, who it claims to be, before granting it access to a protected system or object).

3.4.2. Security Standards Activities

There are a broad spectrum of security requirements for OSI systems, with no one document addressing all the needs for each application or layer. The following documents represent major work in progress in Network Management security.

The Authentication Framework document (CD 10181-2), being produced within ISO/IEC SC 21 WG1, specifies methods for implementing authentication, but this Framework does not specify the protocols to use. This document:

- defines the basic concepts for authentication,
- identifies the possible classes of authentication,
- defines the services used for those classes of authentication mechanisms,
- identifies functional requirements for protocols to support those classes of authentication mechanisms,
- identifies cryptographic techniques to protect authentication information,
- identifies management requirements to support those classes of authentication mechanisms, and
- describes key distribution and key management.

This document is expected to reach IS status in 1992.

The Access Control Framework document (CD SC21 N5529), being produced within ISO/IEC SC 21 WG1, describes four access control policies: identity-based, administratively-imposed, rule-based, and user-selectable. This document also describes three types of access control mechanisms: Access Control Lists (ACL), Capabilities, and Security Labeling. This document is expected to reach IS status in 1992.

Framework documents dealing with non-repudiation, confidentiality, and integrity are also expected in the near future and will be addressed in the GNMP as they progress to IS status.

The security management rapporteur of SC21 WG4 (Security Management) is producing the document, "Objects and Attributes for Access Control" (CD 10164-9). This proposed standard addresses access control for a management association, for management operations, and for notifications. It is expected to reach IS status in 1992.

3.4.3. Authentication

Various standards bodies are developing specifications for incorporating security services within OSI protocols. As appropriate specifications emerge they will be applied to network management and other application layer protocols. To accommodate current security needs prior to standards reaching full

maturity, the GNMP specifies three classes of authentication among which Acquisition Authorities may choose. Specification of security requirements is optional in a Request for Proposal (RFP). If required, the Acquisition Authority shall select only one of the three classes of authentication. These classes provide security (in the form of authentication) in increasing levels, respectively (i.e., class 3 provides more security than class 2, which provides more security than class 1).

All three classes use simple credentials, as defined in the Directory Authentication standard [DDEF], to authenticate an entity requesting the establishment of a management association. The simple credentials structure comprises the following fields: username, password , optional time-stamp, and random number fields. The time-stamp fields and random number fields may be used to protect against replay attacks. A detailed description of each of these classes follows.

Class 1: Class 1 authentication requires use of the username and password fields of the simple credentials. This method uses the extensions to ACSE, ISO/IEC 8650 DAD1 / ISO/IEC 8649 DAD1 (ACSE Authentication Service/Protocol), which define a new functional unit (authentication) in which this information is conveyed in the Protocol Data Unit (PDU). An authenticating entity must compare the username and password against an "authorized users" list to verify the user's identity. If the identity is confirmed, the association is accepted, otherwise it is rejected. The username and password are the minimum amount of information that must be provided for Class 1 authentication. The password is transmitted in the clear, not encrypted in any way. The distribution methods for the usernames and passwords is dependent upon prior agreements between communicating peer entities, and therefore's, beyond the scope of the GNMP.

Class 2: In addition to providing all aspects of Class 1 authentication, Class 2 authentication provides additional security by forming the password using a one-way hash function applied to the authentication information. Optional fields (e.g., the time-stamp or random number field) may be included in the authentication information, to which the hash function is applied, to provide a greater measure of security (i.e., by adding the time-stamp, the password will hash to a different value each time). The hash function to be used in Class 2 authentication is the Data Encryption Standard (DES) used in a one-way mode. This method is independent of a stored cryptographic key. An authenticating entity receives the hashed output in the password field of the simple credentials structure, and then processes the password "known" locally to correspond to the received username (along with the other authentication information as the requesting entity did) through the hash function to produce a test value. This test value and the password field are then checked for equality. If the user identity is authenticated, the association is accepted; otherwise it is rejected. The distribution of the information used as input for hashing is dependent upon prior agreements between communicating peer entities and is therefore beyond the scope of the GNMP.

Class 3: Class 3 provides an even greater level of security than Class 2. Class 3 authentication provides all aspects of class 1 authentication. To achieve the increased level of security, the password is encrypted, using the Data Encryption Standard (DES), with a key known only to the communicating peer entities. Optional information (e.g., a time-stamp or a random number) should be encrypted along with the password (e.g., appended or prepended to the password before application of the encryption function) to provide a greater measure of security (i.e., by adding the time-stamp, the password will not encrypt to the same value each time). An authenticating entity receives the encrypted output in the password field of the simple credentials structure, and then decrypts the password field (using the same secret key) and tests the result for equality to the password "known" locally to correspond to the received username. If the user identity is authenticated, the association is accepted; otherwise it is rejected. The distribution of the key used for encryption is dependent upon prior agreements between authenticating peer entities and is therefore beyond the scope of the GNMP.

3.4.4. Access Control

For the first phase of the GNMP, the access control policy is the following: Once authenticated on an association, an entity shall have access to all management information available through that association. If an entity is not authenticated, it will not be granted an association.

As work progresses on access control in the standards community, access control mechanisms will be added to future phases of the GNMP.

3.4.5. Remaining Services

For the first phase of GNMP, data origin authentication, integrity and confidentiality can not be provided. As work progresses on these services in the standards community, they will be added to future phases of the GNMP.

4. GNMP Specifications

This section contains the specifications for the network management profile. For all NM products to be procured by U.S. Federal Agencies, this GNMP mandates the inclusion of OSI management capabilities which implement: 1) the CMIS/P, as specified in subsection 4.1 of this document, for management communications; 2) the MO definitions, as specified in subsection 4.2, for management information; and 3) the SMFs, as specified in subsection 4.3, for management functions. It is not required that all of the SMFs and MO definitions specified in these subsections be implemented for a particular management product. Rather, it is the responsibility of the Acquisition Authority to specify in each RFP, when procuring NM products, the SMFs and MOs which will satisfy the NM requirements specific to the target network(s). Moreover, when procuring a complete NMS, the Acquisition Authority should take additional steps, as recommended in section 2 of this GNMP, to ensure an adequate specification for the intended use. For example, considerable attention should be given to HMI and analysis needs, since such functionality is usually required.

4.1. Management Communications

A NM implementation shall include the Common Management Information Services and Protocol (CMIS/P) and shall conform to the agreements in part 18 (NM IAs), clause 6 of the OIW Stable IAs, December, 1990 [STABLE]. An implementation shall, also, provide the ACSE services and protocol as specified in the GOSIP Version 2 section 4.2.7.1, as modified by the NMSIG Agreements (part 18 of OIW IAs), clause 6.5. In addition, an implementation shall provide the ROSE services and protocol as specified in the Remote Operations Part 1: Model, Notation and Service Definition [ROSES], and the Remote Operations Part 2: Protocol Specification [ROSEP], and as modified by the NMSIG Agreements clause 6.5. Agreements relating to the presentation and session layers shall also be supported as specified in part 5 (upper layer agreements), clause 13.7 of the OIW Stable IAs, December, 1990 [STABLE]. The particular combination of the allowable layer 1-6 services and protocols selected to support CMIS/P protocols/options shall be dictated by the intended network management applications and by the target network(s).

If VT functionality is required, VT should be employed as specified in the GOSIP Version 2 section 4.2.7.4 [GOSIP].

If FTAM functionality is required, FTAM should be employed as specified in the GOSIP Version 2 sections 4.2.7.2 and 5.3.1 [GOSIP].

If MHS functionality is required, MHS should be employed as specified in the GOSIP Version 2 sections 4.2.7.3, and 5.3.2 [GOSIP].

4.2. Management Information

A NM implementation shall support the agreements specified in part 18 (NM IAs), clause 7.1, 7.2, and 7.3 of the OIW Stable IAs, December, 1990 [STABLE]. In order to support interoperable network management, a set of MOs must be specified for inclusion in a RFP for procuring NM products. Where applicable, MOs shall be selected from the MO definitions in the following documents:

- DMI [DMI]
- Annex A of part 18 (NM IAs) of OIW Working IAs, December 1990 [WORK]
- NMSIG 90/197 [NM802]

- IEEE 802.3 HUB Management [HUB]
- ANSI X3T9.5 FDDI SMT [FDDI]
- ANSI T1M1.5 Telecomm. MOs [T1M1]
- ISO/IEC SC6 Network Layer MOs [SC6]
- Modem MOs [MODEM]

When specifying MOs in a RFP for NM products, the Acquisition Authority must take care to specify: 1) whether optional attributes and/or conditional package(s) are mandatory for the procurement, and 2) from which document the MOs are selected, since some of the MOs have redundant names with either similar or different definitions in other documents. In those cases where applicable MOs are not defined in the above listed documents for managing particular network component(s) or system(s), additional management information definitions may be specified. However, to achieve uniformity in the definition of management information, thus aiding the development of automated tools, such management information should be defined using the techniques and templates as specified in GDMO, and further constrained by part 18 (NM IAs), clause 7 of the OIW Stable IAs, December, 1990 [STABLE]. All MO definitions must have registered object identifiers. Implementors are encouraged to place new MO definitions into standard libraries, whenever possible, to further promote interoperability.

4.3. Systems Management Functions and Services

A NM implementation shall support the agreements in part 18 (NM IAs), clause 5 of the OIW Stable IAs, December, 1990 [STABLE]. When specifying SMFs in an RFP for NM products. the Acquisition Authority must take care to select the applicable SMFs. The Acquisition Authority, then, when specifying the selected SMFs in the RFP, shall also specify the selected functional units, and whether conformance to the agent role or conformance to the manager role or both is required.

4.4. Security Options

Peer entity authentication, an Application Layer function, shall be performed during association establishment, and shall be accomplished using ACSE extensions ISO/IEC 8650/DAD1 and ISO/IEC 8649/DAD1 [ACSE1][ACSE2]. These extensions define a new functional unit and associated ASN.1 definition of an "authentication" parameter to support authentication. If any class of authentication is selected for use by the Acquisition Authority, the vendor must implement the two ACSE addenda [ACSE1][ACSE2]. In addition, the implementation shall utilize SimpleCredentials as defined in the Directory Authentication Framework Part 3 [DDEF], for use in the authentication field of the protocol addenda [ACSE2]. The implementation must follow the method of simple authentication as defined in the Directory Authentication Framework Part 8, Section 2 [DAUTH]. The authentication (checks for equality) performed by The Directory in section 2 must be performed by the authenticating entity, since use of The Directory is not mandatory. In all authentication classes, password usage must conform to FIPS 112, Password Usage [PASS]. In all classes, the distribution of the usernames and passwords is dependent on prior agreements between authenticating peer entities and is therefore beyond the scope of this document.

Class 1 For this class of authentication, the password is sent in the clear, not encoded in any way. Use of the username and password fields is mandatory, the time-stamp and random number fields are optional.

Class 2 In addition to providing all aspects of Class 1 authentication, Class 2 authentication provides additional security by forming the password using a one-way hash function applied to the authentication information. The hashing function and its use is defined in FIPS 112, Password Usage, appendix D [PASS]. The distribution of the information used for hashing (authentication information) is dependent upon prior agreements between authenticating peer entities and is therefore beyond the scope of this document.

Class 3 Class 3 authentication provides all aspects of class 1 authentication. To achieve an increased level of security, the password is encrypted, using the Data Encryption Standard (DES). Encryption will be performed in accordance with the Data Encryption Standard, FIPS 46-1 [DES]. A time variant parameter shall be used in the encryption of the password so as to detect the playback of a previously transmitted encrypted password. (See ANSI X9.26-1990 [TECH] for examples of password encryption techniques). Cryptographic modules must comply with the security requirements specified in FIPS PUB 140-1 [CRYPT]. The distribution of the key used for encryption is dependent upon prior agreements between authenticating peer entities and is therefore beyond the scope of this document.

Inclusion of these security specifications in an RFP is optional.

5. Conformance and Interoperability Testing

5.1. Conformance Requirements

Implementations may be conformant to the Government Network Management Profile in any of three areas: management communications, management information, and systems management functions. An implementation may be conformant to one or more of these areas.

Note: When purchasing implementations, Acquisition Authorities shall specify the areas to which conformance is required.

To be conformant with the Government Network Management Profile in the area of management communications, an implementation shall satisfy the requirements for management communications as stated in section 4.1.

To be conformant with the Government Network Management Profile in the area of management information (managed object classes), an implementation shall satisfy the requirements for management information as stated in section 4.2. Implementations may be conformant to one or more managed object classes.

Note: As stated in section 4.2, Acquisition Authorities shall specify which managed object classes and conditional packages are required.

To be conformant with the Government Network Management Profile in the area of systems management functions, an implementation shall satisfy the requirements for systems management functions as stated in section 4.3.

Note: As stated in section 4.3, Acquisition Authorities shall specify which systems management functions, functional units, and roles are required.

> **Temporary Note: As this proposed GNMP is being written, it is anticipated that the conformance clauses of CMIP and the SMFs will change significantly in progressing to International Standards (ISs) at the May/June 1991 editing meetings of ISO/IEC JTC1 SC21 in France. If these changes occur, GNMP sections 4 and 5 regarding management communications and SMF conformance will be harmonized with the new International Standards.**

5.2. Conformance Testing

Currently, aside from the components that are common with the GOSIP, there are no conformance tests available for the GNMP. However, conformance testing for management communications (CMIP) is expected to be available by the time that the GNMP is mandatory for procurements.

With respect to other aspects of the GNMP (i.e., systems management functions, managed object classes, and security), it is not likely that conformance tests will be available at the time that the GNMP becomes mandatory for procurements. Therefore,

> **For the interim, the Acquisition Authority shall require that vendors substantiate any claim of conformance for those aspects of the GNMP for which tests are not available.**

5.3. Interoperability Testing

Interoperability testing for the GNMP should be strongly considered. Possibilities for such testing include the use of commercially available interoperability testing services, OSINET, or on-site multi-vendor testing to assure interoperability.

6. References

[ACSE1] "*Information technology - Open Systems Interconnection - Service Definition for the Association Control Service Element, Addendum 1: Peer-entity Authentication during Association Establishment*", ISO/IEC 8649 1988/DAD1.

[ACSE2] "*Information technology - Open Systems Interconnection - Protocol Specification for the Association Control Service Element, Addendum 1: Peer-entity Authentication during Association Establishment*", ISO/IEC 8650 1988/DAD1.

[ALS] "*Information technology - Open Systems Interconnection - Application Layer Structure*", ISO/IEC 9545, September 1988.

[ARF] "*Information technology - Open Systems Interconnection - Systems Management - Part 4: Alarm Reporting Function*", ISO/IEC DIS 10164-4, ISO/IEC JTC1/SC21 N4858, June 1990.

[ARR] "*Information technology - Open Systems Interconnection - Systems Management - Part 3: Attributes for Representing Relationships*", ISO/IEC DIS 10164-3, ISO/IEC JTC1/SC21 N 4857), June 1990.

[BRM] "*Information technology - Open Systems Interconnection - Basic Reference Model*", ISO/IEC 7498, 1984.

[CMIP] "*Information technology - Open Systems Interconnection - Management Information Protocol Specification - Common Management Information Protocol*", ISO/IEC 9596-1, ISO/IEC JTC1/SC21 N5303, 24 Nov 1990.

[CMIS] "*Information technology - Open Systems Interconnection - Management Information Service Definition - Common Management Information Service Definition*", ISO/IEC 9595, ISO/IEC JTC1/SC21 N5302, 24 Nov 1990.

[CRYPT] "*Federal Information Processing Standards Publication 140-1, Security Requirements for Cryptographic Modules*", National Institute of Standards and Technology, 1977.

[DAUTH] "*Information Technology - Open Systems Interconnection - The Directory - Part 8: Authentication Framework* ", ISO/IEC 9594-8, 1990.

[DES] "*Federal Information Processing Standards Publication 46, Data Encryption Standard*", National Institute of Standards and Technology, 15 January 1977.

[DDEF] "*Information Technology - Open Systems Interconnection - The Directory - Part 3: Abstract Service Definition*", ISO/IEC 9594-3, 1990.

[DMI] "*Information technology - Open Systems Interconnection - Structure of Management Information - Part 2: Definitions of Management Information*", ISO/IEC DIS 10165-2, ISO/IEC JTC1/SC21 N 4867, June 1990.

[ERMF] "*Information technology - Open Systems Interconnection - Systems Management - Part 5: Event Report Management Function*", ISO/IEC DIS 10164-5, ISO/IEC JTC1/SC21 N4860, June 1990.

[FDDI] Foco, Wayne; "*FDDI Management Information Base*", A proposal from IBM to ANSI X3T9.5 SMT W.G., IBM Communications Architecture, Research Triangle Park, N.C., February 15, 1991.

[FRMWK] "*Information technology - Open Systems Interconnection - Basic Reference Model - Part 4: Management Framework*", ISO/IEC 7498-4 : 1989(E), 1989.

[GDMO] "*Information technology - Open Systems Interconnection - Structure of Management Information - Part 4: Guidelines for the Definition of Managed Objects*", ISO/IEC DIS 10165-4, ISO/IEC JTC1 SC21 N 4852, 15 June 1990.

[GOSIP] "*Federal Information Processing Standards Publication 146, U.S. Government Open Systems Interconnection Profile (GOSIP)*", Version 2.0 , October 1990.

[HUB] *Draft Supplement to IEEE Std. 802.3 : Hub Management*", P802.3.K/D2, September 1990.

[MIL] "*Appendix A - Management Information Library (MIL) of Sec. 18: Network Management, the Working Implementors Agreement (IA) of the OSI Implementors Workshop*" , December 1990.

[MIM] "*Information technology - Open Systems Interconnection - Management Information Services - Structure of Management Information - Part 1: Management Information Model*", ISO/IEC DIS 10165-1, ISO/IEC JTC1/SC21 N5252, June 1990.

[MODEM] "*Modem Managed Object Definitions*", NMSIG-91/014, March 1991.

[NM802] "*NMSIG Contributions to IEEE802*", NMSIG-90/197, November 1990.

[OMF] "*Information technology - Open Systems Interconnection - Systems Management - Part 1: Object Management Function*", ISO/IEC DP10164-1, ISO/IEC JTC1/SC21 N 4855, June 1990.

[PASS] "*Federal Information Processing Standards Publication 112, Password Usage*", National Institute of Standards and Technology, May 1985.

[ROSEP] "*Information technology - Text Communications - Remote Operations Part 2: Protocol Specification* ", ISO/IEC 9072-2 , 19 September 1989.

[ROSES] "*Information technology - Text Communications - Remote Operations Part 1: Model, Notation and Service Definition*", ISO/IEC 9072-1, 19 September 1989.

[SC6] "*Information technology - Telecommunications and information exchange between systems -- Elements of Management Information Related to OSI network Layer Standards*", ISO/IEC CD 10733, November 1990.

[SMO] "*Information technology - Open Systems Interconnection - Systems Management Overview*", ISO/IEC DIS 10040, ISO/IEC JTC1/SC21 N4865R, 16 June 1990.

[STABLE] NIST Special Publication 500-162, "*Stable Implementation Agreements for Open Systems Interconnection Protocols, Version 3.*" This document can be purchased from National Technical Information Service (NTIS), U. S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161. For telephone orders call: (703) 487-4650.

[STMF] "*Information technology - Open Systems Interconnection - Systems Management - Part 2: State Management Function*", ISO/IEC DIS 10164-2, ISO/IEC JTC21 N 4856, June 1990.

[TECH] "*Financial Institution Sign-On Authentication for Wholesale Financial Transactions*", ANSI X9.26, 1990.

[T1M1] "*American National Standard for Telecommunications - Operations, Administration, Maintenance, and Provisioning - Generic Network Model for Interfaces Between Open Systems and Network Elements*", ANSI T1.214-1990.

[WORK] "*Working Implementation Agreements for Open Systems Interconnection Protocols*", NISTIR-4302.

7. Appendices

A. Advanced Requirements

This appendix provides a forward pointer to additional work planned for the subsequent phases of the GNMP.

A.1. Management Information

The Phase 1 GNMP focuses on identifying the information required for managing implementations incorporating the functionalities specified for layers 1-2 of the OSI Reference Model.

The second phase of the GNMP, planned to be proposed a year after the Phase 1 GNMP is promulgated, will include the information required for managing implementations of the functions specified for layers 3- 7 of the OSI reference model. Phase 3, planned to be proposed a year after the Phase 2 GNMP is published, will specify the management information required for the management of computer applications and services that are outside of the 7-layer communications stack, such as computer operating systems, and database management systems.

An outline of the three phases of management information is presented in Table 1.

Table 1

Categories of Management Information To Be Included in Each Phase of the GNMP

Phase I	Phase II	Phase III
802.X	Protocol Software	Applications
X.25	(Layers 3-7)	Services
ISDN	Routers	Operating Systems
FDDI	Terminal Servers	Computers
Modems	MTAs	Networks
Multiplexors	PBX	Database Management Systems
Bridges	Circuit switches	
Physical Link		

A.2. Systems Management Functions

The inclusion of the Systems Management Functions (SMFs) for subsequent phases of the GNMP is to be in accordance with the status of the management standards. Those SMFs that are already DISs (e.g., the Log Control Function) and the SMFs that are projected to become DISs (e.g., Security Audit Trail Function) in 1991, are likely to be included in Phase 2 of the GNMP.

A.3. Security

The documents mentioned in section 3.4.2 represent most of the major work currently in progress regarding systems management security. Work on Access Control, Confidentiality, Integrity and Nonrepudiation documents are still in their infancy, and could not be included before the publication of this phase, but will be addressed in future phases of the GNMP. The goal of the GNMP is to provide all necessary security services to address the needs in network management.

A.4. The Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) is widely implemented and is likely to be deployed to manage routers. In such deployments, SNMP can be viewed, analogous to proprietary local area network management protocols, as an internetwork management protocol (i.e., for managing sets of routers). Thus, the SNMP can be fitted into a network management architecture that also includes the GNMP protocols. Providing such a capability (i.e., to integrate the GNMP and the SNMP into a single network management system) is a future work item for the GNMP.

B. Acronyms

ACL	Access Control List
ACSE	Association Control Service Element
AE	Application Entity
AMF	Accounting Metering Function
ANSI	American National Standards Institute
ARF	Alarm Reporting Function
ARR	Attributes for Representing Relationships
ASE	Application Service Element
ASN	Abstract Syntax Notation
CD	Committee Draft
CMIP	Common Management Information Protocol
CMIS	Common Management Information Services
DES	Data Encryption Standard
DIS	Draft International Standard
DMI	Definition of Management Information
ERF	Event Report Function
FDDI	Fiber Distributed Data Interface
FIPS	Federal Information Processing Standard
FTAM	File Transfer, Access, and Management
GDMO	Guidelines for the Definition of Managed Objects
GNMP	Government Network Management Profile
GOSIP	Government Open Systems Interconnection Profile
HMI	Human Machine Interface
IA	Implementor's Agreement
IEEE	Institute of Electrical and Electronic Engineers
IS	International Standard
ISDN	Integrated Services Digital Network
ISO/IEC	International Organisation for Standardisation/International Electrotechnical Committee
LAN	Local Area Network
LCF	Log Control Function
MAC	Medium Access Control
MHS	Message Handling Systems
MIL	Management Information Library
MIM	Management Information Model
MSF	Measurement Summarization Function
MUX	Multiplexor
NIST	National Institute of Standards and Technology
NM	Network Management

NMS	Network Management System
NMSIG	Network Management Special Interest Group
OAAC	Objects and Attributes for Access Control
OIW	OSI Implementors Workshop
OMF	Object Management Function
OSI	Open Systems Interconnection
PBX	Private Branch Exchange
PABX	Private Automated Branch Exchange
RFC	Request For Comments
RFP	Request For Proposal
SARF	Security Alarm Reporting Function
SATF	Security Audit Trail Function
SF	Summarization Function
SIG	Special Interest Group
SMAE	Systems Management Application Entity
SMFs	Systems Management Functions
SMFAs	Specific Management Functional Areas
SMI	Structure of Management Information
SMO	Systems Management Overview
SNMP	Simple Network Management Protocol
STMF	State Management Function
TMF	Test Management Function
TP	Transaction Processing
VT	Virtual Terminal
WAN	Wide Area Network
WD	Working Document
WMF	Workload Monitoring Function

C. Managed Objects and Attributes

The following tables list the name of the Managed Objects and their attributes included in Version 1 of the GNMP.

C.1. NMSIG MIL Managed Objects

Managed Object	Attributes	Reference
nmsig-agent	nmsig-agentId	NMSIG MIL Annex A.4.1
nmsig-computerSystem	nmsig-systemId *administrativeState *operationalState *usageState *managementState nmsig-systemTime nmsig-peripheralNames nmsig-userFriendlyLabel	NMSIG MIL Annex A.4.2
nmsig-coTransportProtocolLayerEntity	nmsig-coTransportProtocolLayerEntityId *administrativeState *operationalState *usageState *managementState nmsig-localTransportAddresses nmsig-maxConnections nmsig-openConnections *outgoingConnectionsRequestCounter *incomingConnectionsRequestCounter *outgoingConnectionRejectErrorCounter *incomingConnectionRejectErrorCounter *outgoingDisconnectErrorCounter *incomingDisconnectErrorCounter *incomingDisconnectCounter *outgoingDisconnectCounter *octetsSentCounter *octetsReceivedCounter *incomingProtocolErrorCounter *outgoingProtocolErrorCounter nmsig-checksumTPDUsDiscardedCounter nmsig-transportEntityType nmsig-entityUpTime	NMSIG MIL Annex A.4.3
nmsig-network	nmsig-networkId nmsig-networkPurpose nmsig-userFriendlyLabel	NMSIG MIL Annex A.4.6
nmsig-processingEntity	nmsig-cPU-Type nmsig-memorySize nmsig-osInfo nmsig-entityUpTime *processingErrorAlarm	NMSIG MIL Annex A.4.7

* - ["Recommendation X.721" | "ISO/IEC DIS 10165-2" :]

Managed Object	Attributes	Reference
nmsig-clNetworkProtocolLayerEnuty	nmsig-clNetworkProtocolLayerEntityId *administrativeState *operationalState *usageState *managementState nmsig-localNetworkAddresses nmsig-nPDUTimeToLive nmsig-maxPDUSize *pDUsSentCounter *pDUsReceivedCounter nmsig-PDUsForwardedCounter nmsig-PDUsReasmbldOKCounter nmsig-PDUsReasmblFailCounter nmsig-PDUsDiscardedCounter nmsig-networkEntityType nmsig-entityUpTime nmsig-PDUsRedirected nmsig-manufacturerInfo nmsig-productLabel nmsig-release nmsig-serialNumber	NMSIG MIL Annex A.4.4
nmsig-equipment	nmsig-manufacturerInfo nmsig-productLabel nmsig-release nmsig-serialNumber Snmsig-equipmentId *operationalState *administrativeState *usageState *managementState nmsig-locationName nmsig-contactNames nmsig-equipmentPurpose nmsig-vendorName nmsig-userFriendlyLabel	NMSIG MIL Annex A.4.5

* - ["Recommendation X.721" | "ISO/IEC DIS 10165-2" :]

Managed Object	Attributes	Reference
nmsig-transportConnection	nmsig-transportConnectionId nmsig-localTransportConnectionEndpoint nmsig-remoteTransportConnectionEndpoint nmsig-transportConnectionReference nmsig-localNetworkAddress nmsig-remoteNetworkAddress nmsig-inactivityTimeout nmsig-maxPDUSize *pdusSentCounter *pdusReceivedCounter *octetsSentCounter *octetsReceivedCounter *peer nmsig-maxRetransmissions nmsig-retransmissionTimerInitialValue *pdusRetransmittedErrorCounter *pdusRetransmittedErrorThreshold nmsig-octetsRetransmittedErrorCounter	NMSIG MIL Annex A.4.8
nmsig-transportConnectionProfile	nmsig-transportConnectionProfileId nmsig-inactivityTimeout nmsig-maxTPDuSize	NMSIG MIL Annex A.4.9
nmsig-transportConnectionRetransmissionProfile	nmsig-maxRetransmissions nmsig-retransmissionTimerInitialValue	NMSIG MIL Annex A.4.10

* - ["Recommendation X.721" | "ISO/IEC DIS 10165-2" :]

C.2. NMSIG 90/197 Managed Objects

Managed Object	Attributes	Reference
anySAP	serviceUser OperationalState AdministrativeState	NMSIG-90/197
lLC	supportedOptions lLC-Id OperationalState AdministrativeState manufacturerInfo productLabel release serialNumber unrecognizedPDU-Counter bufferProblemCounter	NMSIG-90/197
lSAP	testCommandRecievedCounter testResponseSentCounter lSAP-Id	NMSIG-90/197
nmsig-lEEE-802.3	nmsig-lEEE-802.3Id OperationalState AdministrativeState nmsig-macAddress nmsig-lEEE-802.3State nmsig-multicastAddressList	NMSIG-90/197

Managed Object	Attributes	Reference
nmsig-IEEE-802.3-RCV	nmsig-IEEE-802.3-RCVId OperationalState AdministrativeState nmsig-multicastRcvState PDUsReceivedCounter nmsig-PDUsFCSErrorCounter nmsig-PDUsAlignmentErrorCounter nmsig-enablePromiscuousState OctetsReceivedCounter nmsig-multicastPDUsRcvCounter nmsig-broadcastPDUsRcvCounter nmsig-PDUsInRangeLengthErrorCounter nmsig-PDUsOutRangeLengthErrorCounter nmsig-PDUsTooLongErrorCounter nmsig-internalMACRcvErrorCounter nmsig-sourceAddrLastFCSErrorPDU nmsig-sourceAddrLastAlignmentErrorPDU nmsig-sourceAddrLastInRangeLengthErrorPDU nmsig-sourceAddrLastOutRangeLengthErrorPDU nmsig-sourceAddrLastTooLongErrorPDU nmsig-PDUsInRangeLengthErrorCounter nmsig-PDUsOutRangeLengthErrorCounter nmsig-PDUsTooLongErrorCounter nmsig-internalMACRcvErrorCounter nmsig-FCSErrorThreshold nmsig-alignmentErrorThreshold nmsig-inRangeThreshold nmsig-outRangeThreshold nmsig-frameTooLongThreshold nmsig-internalMACRcvErrorThreshold	NMSIG-90/197

Managed Object	Attributes	Reference
nmsig-IEEE-802.5	nmsig-IEEE-802.5-Id nmsig-IEEE-802.5-macStatus nmsig-IEEE-802.5-errorReportTimerValue nmsig-IEEE-802.5-privateStateParm OperationalState AdministrativeState nmsig-manufacturerInfo nmsig-productLabel nmsig-release nmsig-serialNumber nmsig-IEEE-802.5-individualMACaddress nmsig-IEEE-802.5-functionalAddresses nmsig-IEEE-802.5-groupMACaddress nmsig-IEEE-802.5-una nmsig-IEEE-802.5-ringNumber nmsig-IEEE-802.5-physicalDrop nmsig-IEEE-802.5-privateAddressParm nmsig-IEEE-802.5-authorizedFunctionClass nmsig-IEEE-802.5-functionalAddresses nmsig-IEEE-802.5-authorizedAccessPriority nmsig-IEEE-802.5-productInstanceID nmsig-IEEE-802.5-privateAttachParm nmsig-IEEE-802.5-lineError nmsig-IEEE-802.5-burstError nmsig-IEEE-802.5-acError nmsig-IEEE-802.5-abortTransError nmsig-IEEE-802.5-internalError nmsig-IEEE-802.5-privateErrorCounters nmsig-IEEE-802.5-lostErameError nmsig-IEEE-802.5-receiveCongestion nmsig-IEEE-802.5-frameCopiedError nmsig-IEEE-802.5-tokenError nmsig-IEEE-802.5-privateErrorCounters	NMSIG-90/197

Managed Object	Attributes	Reference
oBridge	aBridgeAddress aBridgeName aBridgeNumPorts aBridgePortAddresses aBridgeUpTime aBridgeSpanPriority aBridgeSpanTimeSinceTopologyChange aBridgeSpanTopologyChangeCount aBridgeSpanTopologyChangeFlag aBridgeSpanDesignatedRoot aBridgeSpanRootCost aBridgeSpanRootPort aBridgeSpanMaxAge aBridgeSpanHelloTime aBridgeSpanForwardDelay aBridgeSpanBridgeMaxAge aBridgeSpanBridgeHelloTime aBridgeSpanBridgeFwdDelay aBridgeSpanHoldTime aBridgeSRBridgeSize aBridgeSRBridgeNum aBridgeSRRDLimit aBridgeSRRERTimer aBridgeSRRetryCnt	NMSIG-90/197
oBridgeFilteringDB	aBridgeFDBID aBridgeFDBMaxSize aBridgeFDBNumStatic aBridgeFDBNumDynamic	NMSIG-90/197
oBridgeFilteringDBEntry	aBridgeFDBEntryMacAddr aBridgeFDBEntryType aBridgeFDBEntryPortNumber aBridgeFDBAgeingTime aBridgeFDBEntryOutboundPorts	NMSIG-90/197
oBridgePermDB	aBridgePDBID aBridgePDBMaxSize aBridgePDBNumEntries	NMSIG-90/197
oBridgePermDBEntry	aBridgePDBEntryMacAddr aBridgePDBEntryPortNumber aBridgePDBEntryOutboundPorts	NMSIG-90/197
oBridgePortTable	aBridgePortTableID	NMSIG-90/197

Managed Object	Attributes	Reference
oPortEntry	aPortNumber aPortName aPortType aPortUserPriority aPortAccessPriority aPortFramesFwdDiscardsIn aPortFramesRecv aPortFramesForwarded aPortFramesDiscardNoBuffer aPortFramesDiscardTransDelay aPortFramesDiscardOnError aPortFramesDiscardOnErrorDetail aPortSpanUpTime aPortSpanPriority aPortSpanState aPortSpanPathCost aPortSpanDesignatedRoot aPortSpanDesignatedCost aPortSpanDesignatedBridge aPortSpanDesignatedPort aPortSpanTopChangeACK aPortSRSegmentNum aPortSRAPESent aPortSRAPERecv aPortSRSpecSent aPortSRSpecRecv aPortSRNonRoutedSent aPortSRNonRoutedRecv aPortSRSTESent aPortSRSTERecv aPortSRRingMismatch aPortSRBridgeMismatch	NMSIG-90/197

C.3. ISO/IEC SC6 Managed Objects

Managed Object	Attributes	Reference
cLNS	cLNS-MO-Name segmentsReceived segmentsDiscarded expiredSegmentsDiscarded errorReportsReceived pDUFormatErrors unsupportedOptions otherErrors enableChecksum	CD10733 Section 5.5
circuit	circuit-MO-Name *operationalState *administrativeState sN-SAP sN-ServiceProvider holdingTimerMultiplier defaultESConfigTimer activeESConfigTimer iSReachabilityChanges iSConfigurationTimer suggestedESConfigurationTimer redirectHoldingTime eSReachabilityChanges manualISDTEAddress callsPlaced callsFailed initialMinimalTimer reserveTimer idleTimer manualISAddress manualISDTEAddress callsPlaced callsFailed manualISDTEAddress	CD10733 Section 5.6
nSAP	nSAP-MO-Name networkEntityRelationship transportClientRelationship	CD10733 Section 5.4
networkEntity	networkEntity-MO-Name networkEntityTitles	CD10733 Section 5.3
networkSubsystem	networkSubsystem-MO-Name	CD10733 Section 5.2
cONS	cONS-MO-Name *operationalState *administrativeState	CD10733 Section 5.7

* - ["Recommendation X.721" | "ISO/IEC DIS 10165-2" :]

Managed Object	Attributes	Reference
x25PLE	x25PLE-MO-Name *operationalState *administrativeState protocolVersionSupported localDTEAddress interfaceMode maxActiveCircuits restartTime minimumRecallTimer restartCount datalinkID logicalChannelAssignments extendedPacketSequencing *octetsSentCounter *octetsReceivedCounter dataPacketsSent dataPacketsReceived callAttempts callsConnected providerInitiatedDisconnects callTimeouts clearTimeouts remotelyInitiatedResets dataRetransmissionTimerExpiries providerInitiatedResets resetTimeouts remotelyInitiatedRestarts restartTimeouts protocolErrorsDetectedLocally protocolErrorsAccusedOf retryCountsExceeded clearCountsExceeded interruptPacketsSent interruptPacketsReceived interruptTimerExpiries pLEClientMOName	CD10733 Section 5.8

* - ["Recommendation X.721" | "ISO/IEC DIS 10165-2" :]

Managed Object	Attributes	Reference
x25PLEIVMO	x25PLEIVMO-Name localDTEAddress interfaceMode maxActiveCircuits restartTime registrationRequestTime minimumRecallTimer restartCount registrationRequestCount dataLinkID logicalChannelAssignments extendedPacketSequencing	CD10733 Section 5.9
iSO8208VirtualCallIVMO	iSO8208Virtual-Call-IVMO-Name proposedPacketSize proposedWindowSize acceptReverseCharging proposeReverseCharging fastSelect callTime resetTime clearTime interruptTime resetCount clearCount logicalChannelAssignments windowTime dataRetransmissionTime dataRetransmissionCount rejectTime rejectCount	CD10733 Section 5.10

Managed Object	Attributes	Reference
virtualCall	virtualCall-MO-Name channel packetSize windowSize *octetsSentCounter *octetsReceivedCounter dataPacketsSent dataPacketsReceived remotelyInitiatedResets dataRetransmissionTimerExpiries providerInitiatedResets resetTimeouts interruptPacketsSent interruptPacketsReceived interruptPacketsExpiries	CD10733 Section 5.11
switchedVirtualCall	virtualCall-MO-Name channel packetSize windowSize *octetsSentCounter *octetsReceivedCounter dataPacketsSent dataPacketsReceived remotelyInitiatedResets dataRetransmissionTimerExpiries providerInitiatedResets resetTimeouts interruptPacketsSent interruptPacketsReceived interruptPacketsExpiries direction calledDTEAddress callingDTEAddress callData throughputClass redirectReason originallyCalledAddress callingAddressExtension targetAddressExtension	CD10733 Section 5.12

* - ["Recommendation X.721" | "ISO/IEC DIS 10165-2" :]

Managed Object	Attributes	Reference
permanentVirtualCircuit	virtualCall-MO-Name channel packetSize windowSize *octetsSentCounter *octetsReceivedCounter dataPacketsSent dataPacketsReceived remotelyInitiatedResets dataRetransmissionTimerExpiries providerInitiatedResets resetTimeouts interruptPacketsSent interruptPacketsReceived interruptPacketsExpiries	CD10733 Section 5.13

* - ["Recommendation X.721" | "ISO/IEC DIS 10165-2" :]

C.4. IEEE802.3 HUB Managed Objects

Managed Object	Attributes	Reference
Hub	HubID HubGroupCapacity TimeSinceHubSystemReset HubResetTimeStamp HubHealthState HubHealthText HubHealthData GroupMap	Hub Management #90/89 Section 1.2.3
ResourceTypeID	ResourceType StandardRevision IEEE802-3LmeOptions ManufacturerID ManufacturerProductID ManufacturerProductVersion	Hub Management #90/89 Section 1.2.4
Relay	RelayID TotalCollisions	Hub Management #90/89 Section 1.2.5
GaugeInitialValue	GaugeIVID IVAveragingPeriod IVNumberOfSamples IVNotificationThreshold IVHysteresisThreshold	Hub Management #90/89 Section 1.2.6
Group	GroupID NumberOfPorts	Hub Management #90/89 Section 1.2.7
Port	PortID PortType PortAdminState AutoPartitionState ReadableFrames ReadableOctets Pygmys Runts FrameCheckSequenceErrors AlignmentErrors FramesTooLong AutoPartitionCount OutOfSpecBitRate LastSourceAddress	Hub Management #90/89 Section 1.2.8
Gauge	GaugeID GaugeValue AveragingPeriod NumberOfSamples NotificationThreshold HysteresisThreshold AttributeAppliedTo	Hub Management #90/89 Section 1.2.9

C.5. ANSI X3T9.5 FDDI Managed Objects

Managed Object	Attributes	Reference
fddiSMT	fddiSMTStationId fddiSMTOpVersionId fddiSMTHiVersionId fddiSMTLoVersionId fddiSMTMAC-Ct fddiSMTNonMaster-Ct fddiSMTMaster-Ct fddiSMTPathsAvailable fddiSMTConfigurationCapabilities fddiSMTConfigPolicy fddiSMTConnectionPolicy fddiSMTReportLimit fddiSMTT-Notify fddiSMTStatusReporting fddiSMTECMState fddiSMTCF-State fddiSMTRemoteDisconnectFlag fddiSMTMsgTimeStamp fddiSMTTransitionTimeStamp fddiSMTManufacturerData fddiSMTUserData fddiSMTSetCount fddiSMTLastSetStationId fddiSMTHoldState	X3T9.5/84-49 (Nov 90) Section 6.4.3.1.1
fddiPATH	fddiPATHClassIndex fddiPATHClassTrace-MaxExpiration FddiPATHVXLowerBound FddiPATHT-MAXLowerBound	X3T9.5/84-49 (Nov 90) Section 6.4.3.1.3
fddiPATHNonLocal	fddiPATHNonLocalIndex fddiPATHPORTOrder fddiPATHStatus fddiPATHConfiguration fddiPATHRingLatency fddiPATHTraceStatus fddiPATHT-Rmode FddiPATHSba FddiPATHSbaOverhead	X3T9.5/84-49 (Nov 90) Section 6.4.3.1.4

Managed Object	Attributes	Reference
fddiMAC	fddiMACIndex fddiMACFrameStatusCapabilities fddiMACT-MaxGreatestLowerBound fddiMACTVXGreatestLowerBound fddiMACPathsAvailable fddiMACCurrentPath fddiMACUpstreamNbr fddiMACOldUpstreamNbr fddiMACDup-Addr-Test fddiMACPathsRequested fddiMACDownstreamPORTType fddiMACSMTAddress fddiMACTReq fddiMACTNeg fddiMACTMax fddiMACTvxValue fddiMACTMin fddiMACFrameStatus fddiMACFrame-Ct fddiMACError-Ct fddiMACLost-Ct fddiMACRMTState fddiMACDa-Flag fddiMACUnaDa-Flag fddiMACFrameMACCondition fddiMACLongAlias fddiMACShortAlias fddiMACLongGrpAddress fddiMACShortGrpAddress fddiMACTvxExpired-Ct fddiMACLate-Ct fddiMACRingOp-Ct fddiMACLLCServiceAvailable fddiMACMasterSlaveLoopStatus fddiMACRootMACDownstreamPORTType fddiMACRootMACCurrentPath FddiMACNotCopied-Ct FddiMACFrameNotCopied-CtCondition FddiMACFrameNotCopiedThreshold FddiMACFrameNotCopiedRatio FddiMACDownstreamNbr FddiMACOldDownstreamNbr FddiMACBridgeFunction	X3T9.5/84-49 (Nov 90) Section 6.4.3.1.2

Managed Object	Attributes	Reference
fddiMAC (Cont'd)	FddiMACBaseNotCopied-Ct FddiMACBaseCopied-Ct FddiMACBaseTimeNotCopied FddiMACPri1 FddiMACPri2 FddiMACPri3 FddiMACPri4 FddiMACPri5 FddiMACPri6 FddiMACPri7	X3T9.5/84-49 (Nov 90) Section 6.4.3.1.2
fddiPORT	fddiPORTIndex fddiPORTPC-Type fddiPORTPC-Neighbor fddiPORTConnectionPolicies fddiPORTRemoteMACIndicated fddiPORTCE-State fddiPORTPathsRequested fddiPORTMACPlacement fddiPORTAvailablePaths fddiPORTMACLoop-Time fddiPORTTB-Max fddiPORTBS-Flag fddiPORTLCTFail-Ct fddiPORTLer-Estimate fddiPORTLem-Reject-Ct fddiPORTLem-Ct fddiPORTBaseLer-Estimate fddiPORTBaseLer-Reject-Ct fddiPORTBaseLem-Ct fddiPORTBaseLer-TimeStamp fddiPORTLer-Cutoff fddiPORTLer-Alarm fddiPORTConnectState fddiPORTPCMState fddiPORTPC-Withold fddiPORTLerCondition fddiPORTFotxClass fddiPORTMainLineState fddiPORTEBError-Ct	X3T9.5/84-49 (Nov 90) Section 6.4.3.1.5
fddiATTACHMENT	FddiATTACHMENTIndex fddiATTACHMENTClass fddiATTACHMENTOpticalBypassPresent fddiATTACHMENTI-MaxExpiration fddiATTACHMENTInsertedStatus fddiATTACHMENTInsertPolicy	X3T9.5/84-49 (Nov 90) Section 6.4.3.1.6

C.6. ANSI T1M1.5 Managed Objects

Managed Object	Attributes	Reference
alarmRecord	logRecordId eventType objectClassOfReference objectOfReference eventTime perceivedSeverity probableCause backUpObjectInstance backUpStatus correlatedRecordName monitoredAttributes problemData problemText proposedRepairAction specificProblem stateChange suspectObjectList thresholdInfo trendIndication	ANSI T1.214-1990 Section 6.1.1
channel	directionality aTermination administrativeState alarmState channelId currentProblemList nextHigherOrderChannel nextLowerOrderChannelList operationalState pathName usageState zTermination	ANSI T1.214-1990 Section 6.1.2
channelTermination	tPDirection adminstrativeState alarmState currentProblemList operationalState supportingEQNameList supportingHWNameList supportingSWNameList usageState channelTerminationId channelName linkedObject nextHigherOrderChannelTermination nextLowerOrderChannelTerminationList	ANSI T1.214-1990 Section 6.1.3

Managed Object	Attributes	Reference
cross-Connection	crossConnectionId administrativeState aP-CTermination alarmState currentProblemList operationalState supportingEQNameList supportingHWNameList supportingSWNameList usageState zP-CTermination	ANSI T1.214-1990 Section 6.1.4
currentAlarmSummaryControl	currentAlarmSummaryControlId alarmStateList objectList perceivedSeverityList probableCauseList	ANSI T1.214-1990 Section 6.1.5
discriminator	adminstrativeState beginTime discriminatorConstruct discriminatorId endTime operationalState weekMask	ANSI T1.214-1990 Section 6.1.6
equipment	equipmentId administrativeState alarmState currentProblemList equipmentCode equipmentFunction locationName operationalState supportingEQNameList supportingHWNameList supportingSWNameList supportsObjectList usageState vendorName	ANSI T1.214-1990 Section 6.1.7
eventForwardingDiscriminator	adminstrativeState beginTime discriminatorConstruct discriminatorId endTime operationalState weekMask destinationAddress	ANSI T1.214-1990 Section 6.1.8

Managed Object	Attributes	Reference
framedPath	directionality aTermination administrativeState alarmState channelNameList currentProblemList lineNameList operationalState pathId supportedServiceNameList usageState zTermination	ANSI T1.214-1990 Section 6.1.9
framedPathTermination	tPDirection adminstrativeState alarmState currentProblemList operationalState supportingEQNameList supportingHWNameList supportingSWNameList usageState framedPathTerminationId framedPathName linkedObject	ANSI T1.214-1990 Section 6.1.10
hardware	hardwareId administrativeState alarmState currentProblemList operationalState release replacementHardwareCode supportingHWNameList supportingSWNameList supportsObjectList usageState vendorName	ANSI T1.214-1990 Section 6.1.11

Managed Object	Attributes	Reference
informationPath	directionality aTermination administrativeState alarmState channelNameList currentProblemList lineNameList operationalState pathId supportedServiceNameList usageState zTermination	ANSI T1.214-1990 Section 6.1.12
informationPathTermination	tPDirection adminstrativeState alarmState currentProblemList operationalState supportingEQNameList supportingHWNameList supportingSWNameList usageState informationPathTerminationId informationPathName linkedObject	ANSI T1.214-1990 Section 6.1.13
line	directionality aTermination administrativeState alarmState currentProblemList firstOrderChannelNameList lineId operationalState pathNameList spanNameList supportedServiceNameList usageState zTermination	ANSI T1.214-1990 Section 6.1.14

Managed Object	Attributes	Reference
lineTermination	tPDirection adminstrativeState alarmState currentProblemList operationalState supportingEQNameList supportingHWNameList supportingSWNameList usageState lineTerminationId firstOrderChannelTerminationList lineName pathTerminationList	ANSI T1.214-1990 Section 6.1.15
log	logId administrativeState beginTime endTime logFullAction operationalState usageState discriminatorConstruct numberOfRecords	ANSI T1.214-1990 Section 6.1.16
logRecord	logRecordId eventType objectClassOfReference objectOfReference eventTime	ANSI T1.214-1990 Section 6.1.17
managementOperationsSchedule	administrativeState affectedObjectClass affectedObjectInstances destinationAddress interval scheduleId beginTime endTime operationalState	ANSI T1.214-1990 Section 6.1.18
network	networkId administrativeState operationalState supportedByObjectList supportedNetworkNameList supportedServiceNameList usageState	ANSI T1.214-1990 Section 6.1.19

Managed Object	Attributes	Reference
networkElement	networkElementId systemTitle administrativeState alarmState currentProblemList operationalState supportingEQNameList supportsObjectList usageState vendorName	ANSI T1.214-1990 Section 6.1.20
path	directionality aTermination administrativeState alarmState channelNameList currentProblemList lineNameList operationalState pathId supportedServiceNameList usageState zTermination	ANSI T1.214-1990 Section 6.1.21
pathGroup	pathGroupId pathGroupType pathNameList administrativeState alarmState currentProblemList operationalState usageState	ANSI T1.214-1990 Section 6.1.22
service	serviceId serviceType administrativeState alarmState currentProblemList operationalState supportedServiceNameList supportedByObjectList usageState	ANSI T1.214-1990 Section 6.1.23
software	softwareId alarmState currentProblemList release supportingEQNameList supportingHWNameList supportingSWNameList supportsObjectList	ANSI T1.214-1990 Section 6.1.24

Managed Object	Attributes	Reference
span	directionality administrativeState aTermination alarmState currentProblemList lineName operationalState spanId usageState zTermination	ANSI T1.214-1990 Section 6.1.25
spanTermination	tPDirection adminstrativeState alarmState currentProblemList operationalState supportingEQNameList supportingHWNameList supportingSWNameList usageState spanTerminationId spanName	ANSI T1.214-1990 Section 6.1.26
terminationPoint	tPDirection adminstrativeState alarmState currentProblemList operationalState supportingEQNameList supportingHWNameList supportingSWNameList usageState	ANSI T1.214-1990 Section 6.1.27
top	objectClass	ANSI T1.214-1990 Section 6.1.28

C.7. Modem Managed Object

Managed Object	Attributes	Reference
nist-Modem	nist-Modem-Id nist-Modem-answer-rings nist-Modem-count-rings nist-Modem-escape-char nist-Modem-carriage-return nist-Modem-line-feed nist-Modem-backspace nist-Modem-wait-time-dial-tone nist-Modem-wait-time-carrier nist-Modem-wait-time-comma nist-Modem-wait-time-recognize nist-Modem-loss-time nist-Modem-touch-tone-speed nist-Modem-escape-guard-time nist-Modem-bit-mapped-register14 nist-Modem-test-modes nist-Modem-test-duration nist-Modem-bit-mapped-register21 nist-Modem-bit-mapped-register22 nist-Modem-bit-mapped-register23 nist-Modem-delay-to-DTR nist-Modem-RTS-to-CTS-delay nist-Modem-bit-mapped-register27	NMSIG-91/014

D. Name Bindings

The following figures show the suggested name bindings of the Managed Objects included in Version 1 of the GNMP.

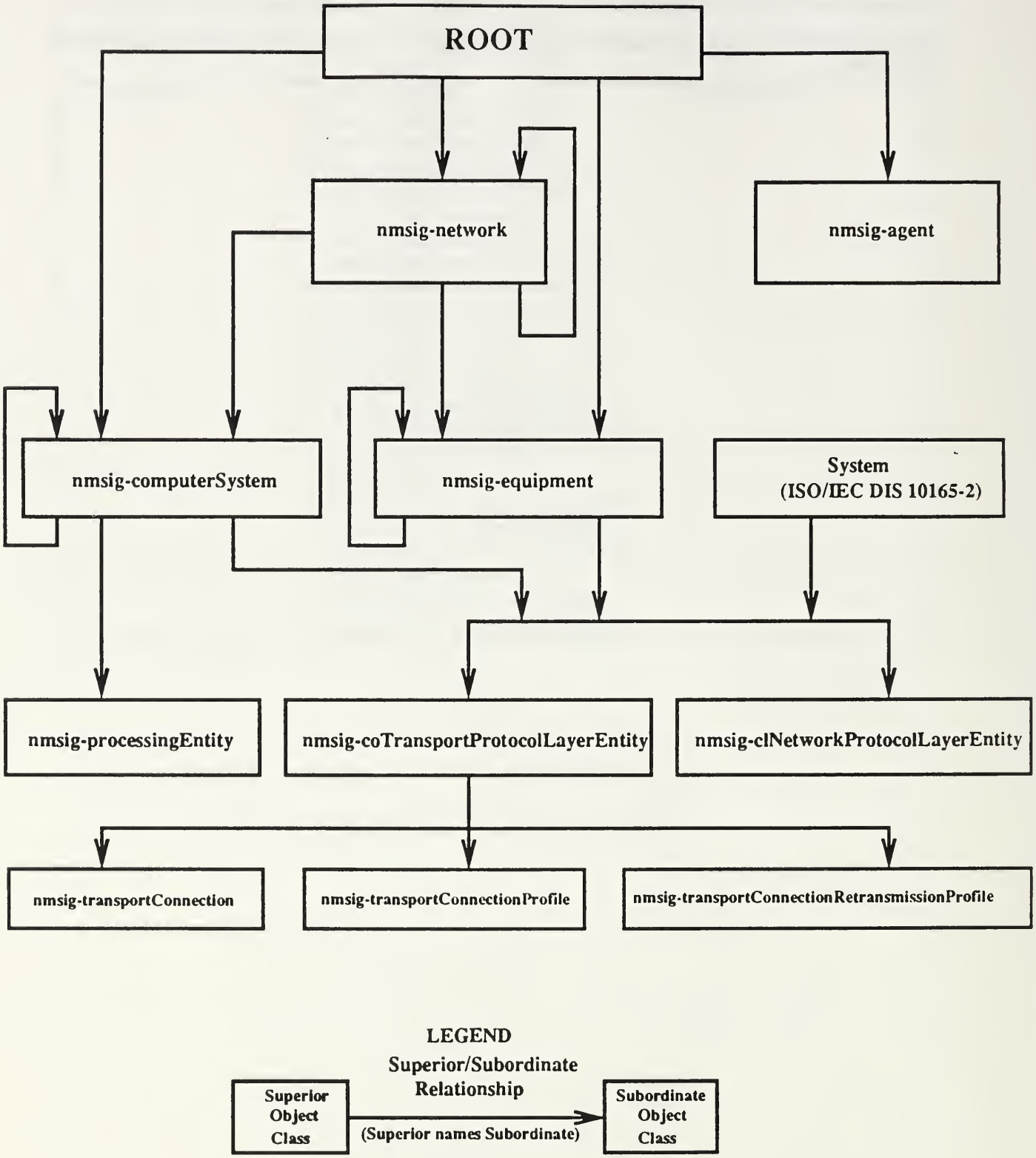


Figure D.1 Name Bindings - NMSIG-MIL Managed Objects

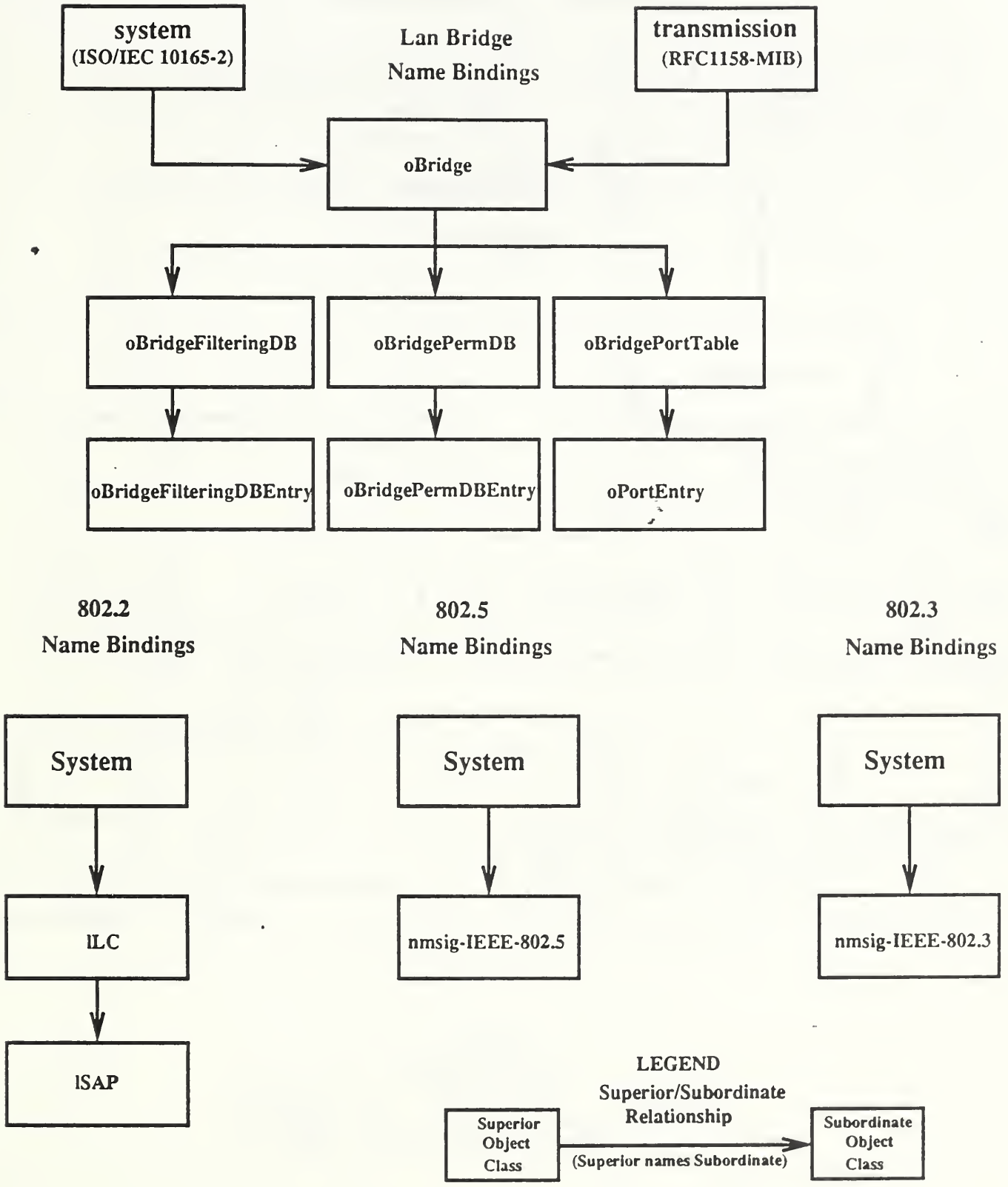


Figure D.2 Name Bindings - NMSIG-90/197 Managed Objects

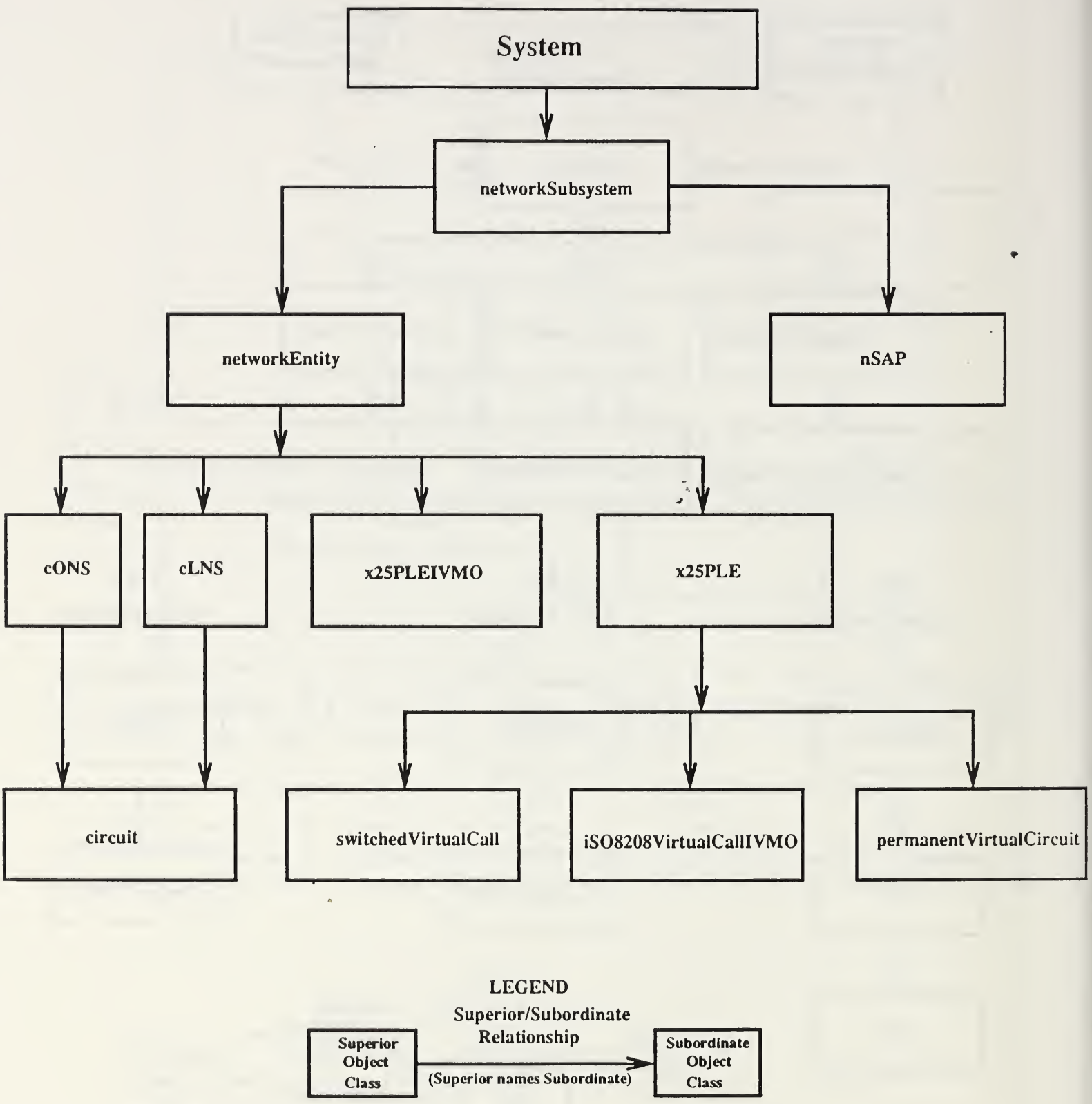


Figure D.3 Name Bindings - ISO SC6 Managed Objects

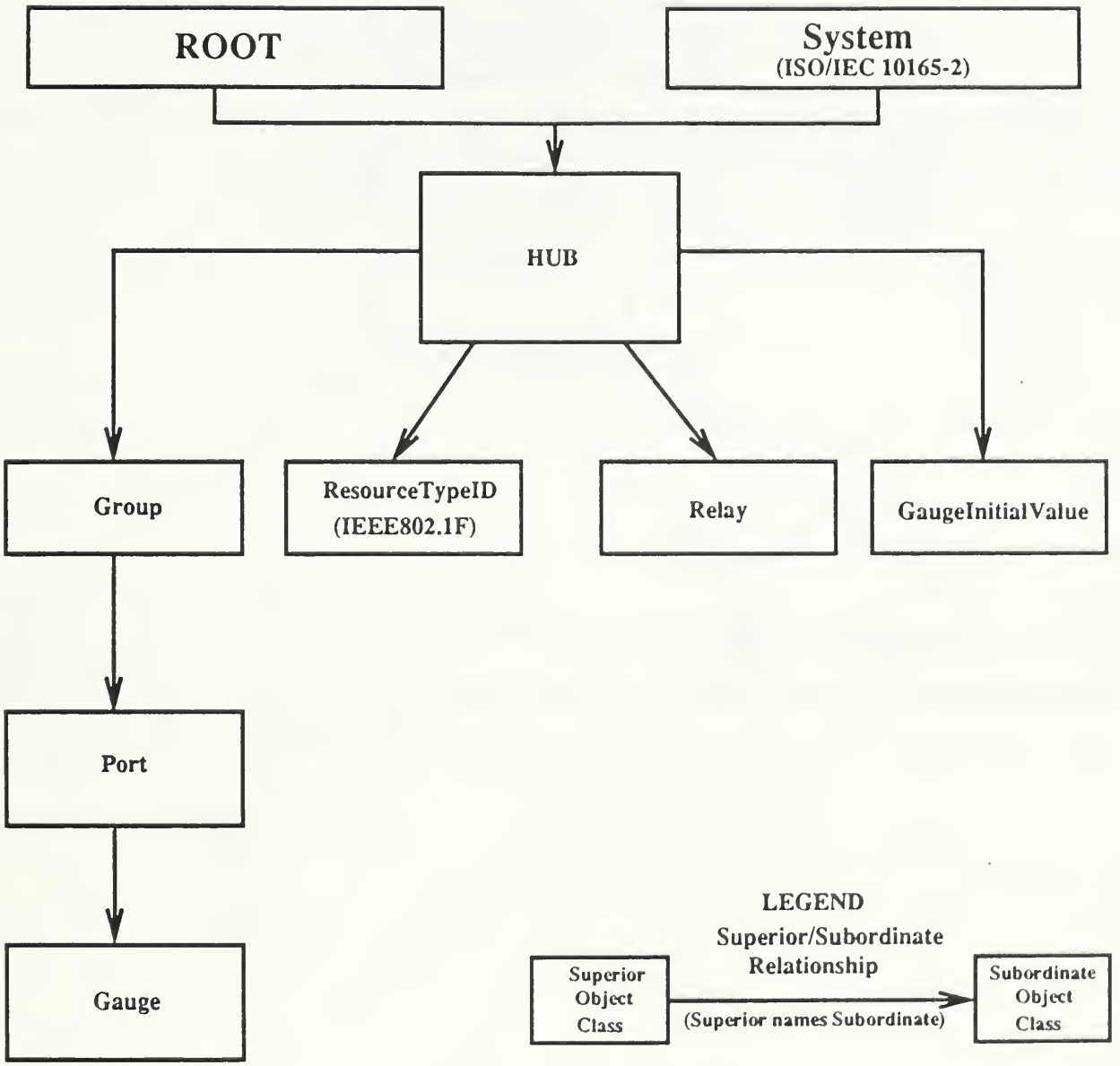


Figure D.4 Name Bindings - IEEE802.3 HUB Managed Objects

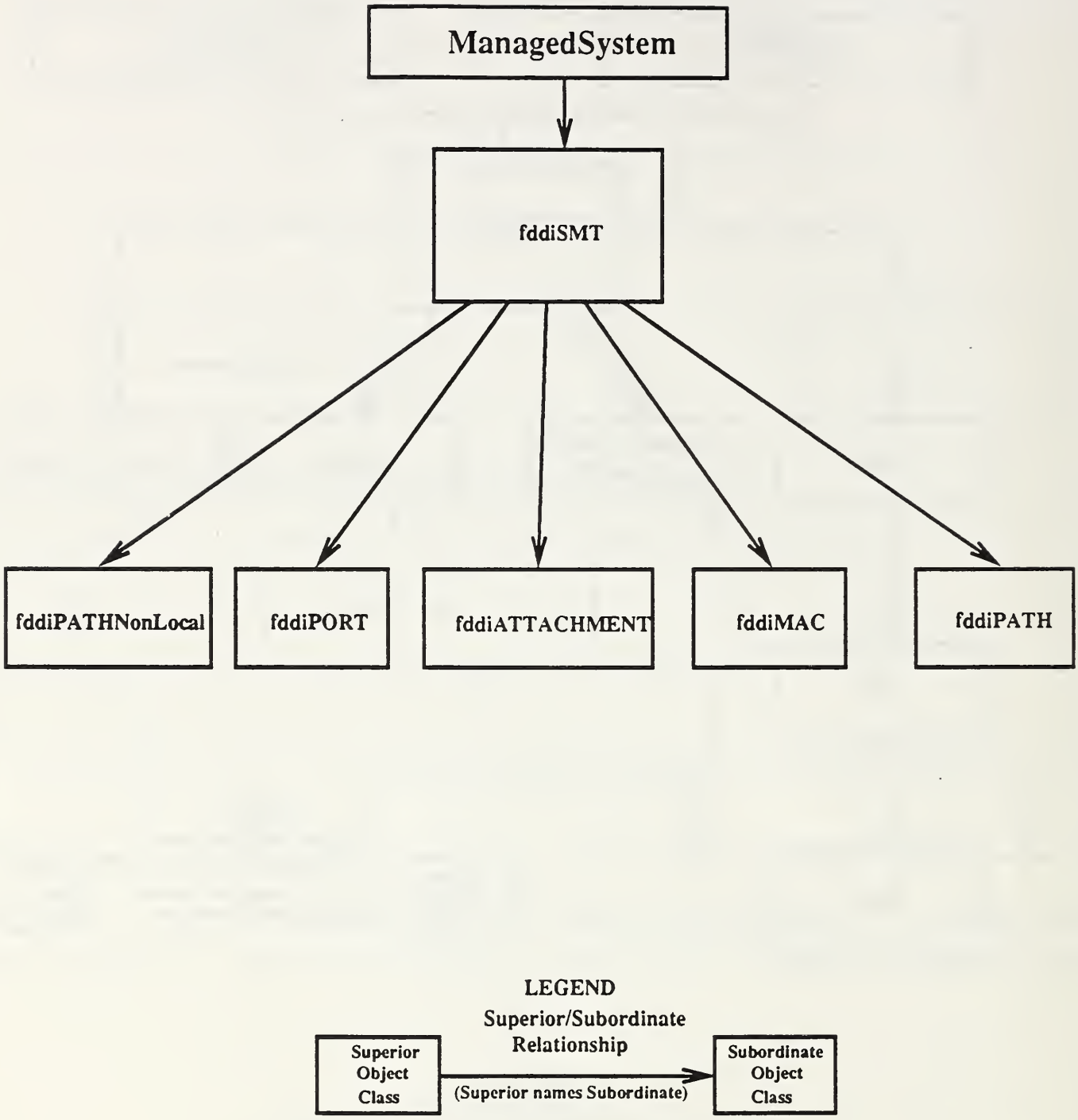


Figure D.5 Name Bindings - ANSI X3T9.5 FDDI Managed Objects

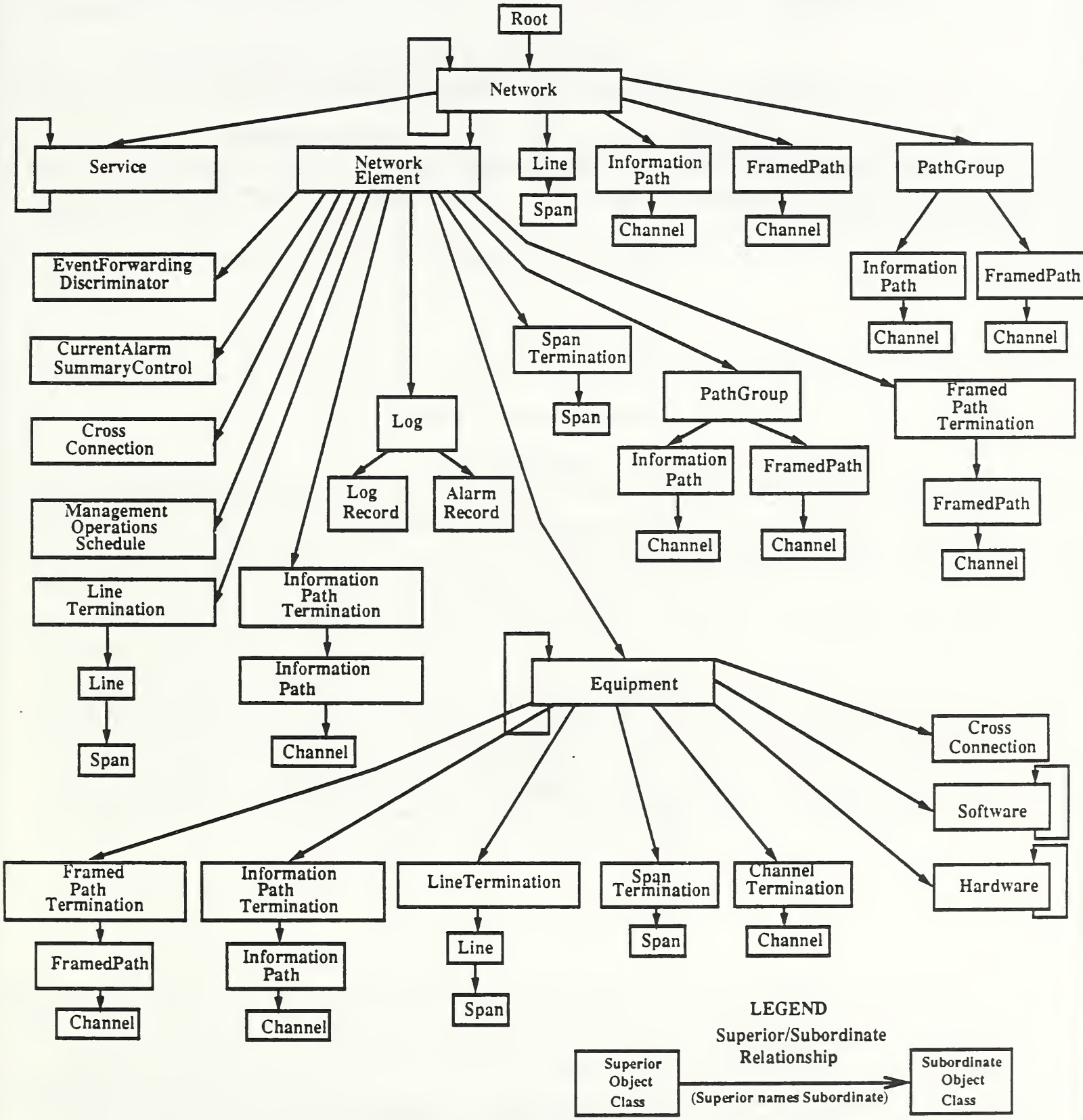
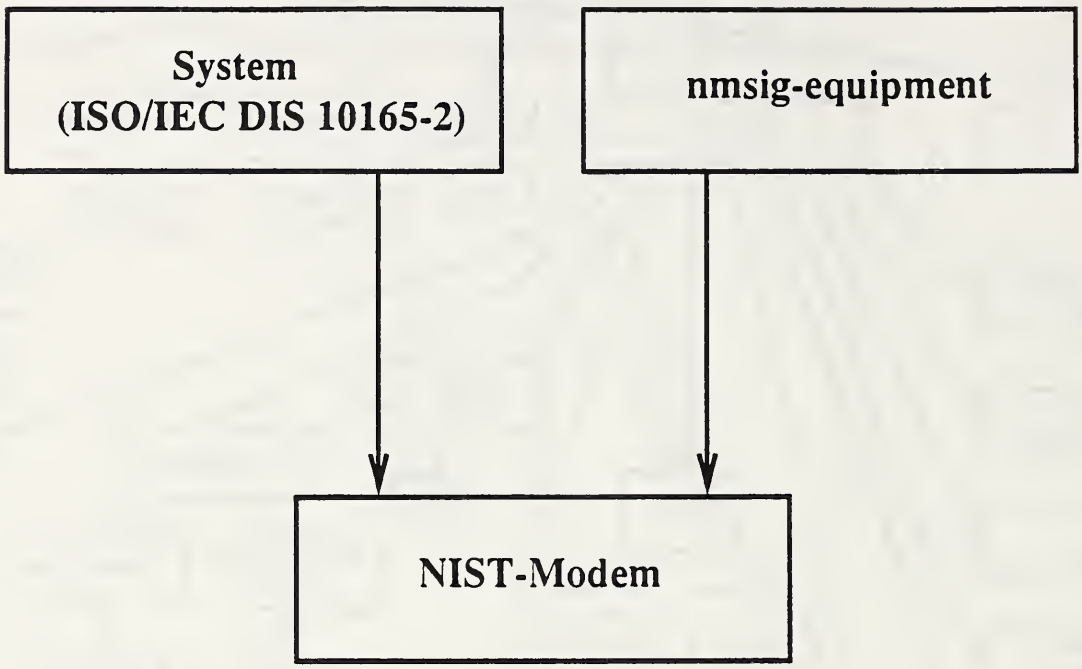


Figure D.6 Name Bindings - ANSI T1M1.5 Managed Objects



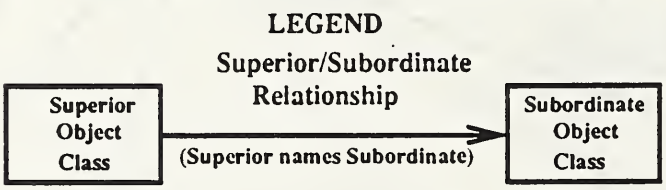


Figure D.7 Name Bindings - Modem Managed Object

NIST-114A
(REV. 3-90)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

BIBLIOGRAPHIC DATA SHEET

1. PUBLICATION OR REPORT NUMBER
NISTIR 4651

2. PERFORMING ORGANIZATION REPORT NUMBER

3. PUBLICATION DATE
JANUARY 1992

4. TITLE AND SUBTITLE

Government Network Management Profile (GNMP):
Public Review Version of Proposed FIPS

5. AUTHOR(S)

6. PERFORMING ORGANIZATION (IF JOINT OR OTHER THAN NIST, SEE INSTRUCTIONS)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
GAITHERSBURG, MD 20899

7. CONTRACT/GRANT NUMBER

8. TYPE OF REPORT AND PERIOD COVERED

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (STREET, CITY, STATE, ZIP)

10. SUPPLEMENTARY NOTES

11. ABSTRACT (A 200-WORD OR LESS FACTUAL SUMMARY OF MOST SIGNIFICANT INFORMATION. IF DOCUMENT INCLUDES A SIGNIFICANT BIBLIOGRAPHY OR LITERATURE SURVEY, MENTION IT HERE.)

The Government Network Management Profile (GNMP) is the standard reference for all Federal Government agencies to use when acquiring Network Management (NM) functions and services for computer and communications systems and networks.

The GNMP is being developed in phases. This document specifies the initial proposed version of the GNMP.

The proposed version 1 GNMP specifies the common management information exchange protocol and services, specific management functions and services, and the syntax and semantics of the management information required to support monitoring and control of network and system components and their resources. Version 1 GNMP also includes optional methods of authentication. These optional authentication methods are provided for interim use in the absence of standard approaches to network management security.

12. KEY WORDS (6 TO 12 ENTRIES; ALPHABETICAL ORDER; CAPITALIZE ONLY PROPER NAMES; AND SEPARATE KEY WORDS BY SEMICOLONS)

Common Management Information Services and Protocol(CMIS/P); Government Network Management Profile(GNMP); Management Security; Managed Objects; Network Management; OSI Network Management Implementors Agreements; OSI Network Management Standards; Systems Management Functions and Services

13. AVAILABILITY

XX	UNLIMITED
	FOR OFFICIAL DISTRIBUTION. DO NOT RELEASE TO NATIONAL TECHNICAL INFORMATION SERVICE (NTIS).
	ORDER FROM SUPERINTENDENT OF DOCUMENTS, U.S. GOVERNMENT PRINTING OFFICE, WASHINGTON, DC 20402.
XX	ORDER FROM NATIONAL TECHNICAL INFORMATION SERVICE (NTIS), SPRINGFIELD, VA 22161.

14. NUMBER OF PRINTED PAGES
72

15. PRICE
A04

ELECTRONIC FORM